Otnetic: A Cyber Range Training Platform Developed for the Norwegian Energy Sector

SINDRE BERGAN & EMIL MORØNNING RUUD

SUPERVISORS

Maung Kyaw Sein & Marko Ilmari Niemimaa

University of Agder, 2021
Faculty of Social Sciences
Department of Information Systems

Acknowledgements

Firstly, we would like to thank our supervisors, Maung Kyaw Sein and Marko Ilmari Niemimaa, for their support and advice.

We would also like to take this opportunity to thank Eva Brekka from NC-Spectrum for being our project client and providing invaluable assistance throughout the project.

We also thank Tom R. Eikebrokk from the Department of Information Systems at UiA for assisting us with the quantitative analysis.

We would like to extend our gratitude to all the people who participated in our lab experiment, and the interview subjects who took time out their day to help us with our project.

Lastly, we would like to thank our family and friends for all their support during this project.

Abstract

As cyber attacks have become increasingly frequent and complex, the need for effective cybersecurity training has become essential. This master thesis was developed in collaboration with the client organization NC-Spectrum, with the objective of developing an alternative training program utilizing cyber ranges and gamified training for OT-personnel in the Norwegian energy sector. The need additional training was identified by the client organization initially, and reinforced through the findings from the literature review and interviews conducted as part of this thesis. Current training methods commonly use one-way communication, which has been shown to be inefficient for facilitating motivation and knowledge retention. As the thesis has employed the design science research method (DSR), an artifact called OTnetic was produced as a result of this thesis. The artifact was created using multiple open source technologies and tools. The requirements for OTnetic, were elicited by analyzing the interviews and creating user stories. OTnetic allows trainees to acquire knowledge and practical skills by completing tasks in a cyber range environment. The cyber range is supplemented with a quiz and information about a given cyber security related question. As the target audience for training in this thesis have been found to have limited cybersecurity knowledge, a module on password security was developed in the first DSR cycle. The entire training program was accessible through the learning management system, Moodle. The artifact was tested by conducting a lab experiment, and evaluated based on a set of pre-defined metrics for evaluating the quality of the software and the training content. Furthermore, the results indicate that gamification and cyber range based training can be an efficient and motivating method to teach cybersecurity to OT-personnel in the Norwegian energy sector. Moreover, OTnetic outperformed lecture-based training when tested by two groups of participants lacking knowledge of cyber security and information technology. The research presented in this thesis can be of great value to companies in the Norwegian energy sector, and contribute to closing the research gap identified in the thesis.

Keywords:

- Cyber Security Training
- Critical Infrastructure
- Energy Sector
- Gamification
- Cyber Ranges
- Design Science Research

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The frequency, sophistication and impact of cyber attacks has increased over the years as adversaries have continued to develop their skills and applied more advanced attack methods, tactics and strategies (Nagarajan, Allbeck, Sood, & Janssen, 2012). Such attacks have the potential to cause great financial losses, and compromise the privacy of user data and the integrity of systems (Kamiya, Kang, Kim, Milidonis, & Stulz, 2018). In order for an organization to be prepared for future threats, training and preparing for a variety of attacks is crucial. Organizations need to not only have technical security controls and a solid security culture, but also train for and simulate cyber attacks in order to prepare for future attacks and stay updated on the current threat landscape. This enables stakeholders to act appropriately in crisis situations. Due to the progressively complex cyber threat landscape, organizations are forced to recognize the importance of a strong cybersecurity posture.

Because cyber threats have become a growing issue for companies where IT plays a strategic role, cybersecurity preparedness has become increasingly salient in the effort to protect the enterprise. Preparedness can be viewed as how an organization reacts to, and prepares for an attack, with the goal of preventing them or mitigating their impact. Effective cybersecurity preparedness requires training and familiarity with the systems that need protection. Furthermore it is necessary to have awareness regarding different types of threats, whether they are malicious, or arise from negligent or oblivious insiders. This is particularly crucial in organizations that develop, operate and maintain critical infrastructure, as they provide society with basic human needs. Critical energy infrastructure (CEI) organizations are particularly attractive targets for terrorists and foreign governments during wartime (Onyeji, Bazilian, & Bronk, 2014). Therefore, these it is crucial that these organizations are sufficiently protected.

Cyber attacks are a new and emerging threat to critical infrastructure sectors, which historically have more experience with physical attacks (MacKinnon et al., 2013). Attacks on monitoring and security equipment using Distributed Denial of Service (DDoS) attacks to shut down systems and malware attacks have been used against energy companies in the past (MacKinnon et al., 2013). Onyeji et al. (2014) refer to this as cyber-enabled physical attacks, a class of cyber-physical threats that use virtual attacks to facilitate physical damage on critical infrastructure. Despite this threat to the energy sector, OT-personnel (operational technology) and industrial control systems (ICS) maintenance staff generally lack awareness of information technology and cybersecurity (Onyeji et al., 2014). The potential impact of cyber attacks in the energy sector necessitates a form of cybersecurity training that is effective and engaging for employees who do not work directly with cybersecurity or information technology. Cyber ranges offer this opportunity, but current research is lacking solutions tailored for users with little prior knowledge about information security. A cyber range is a realistic simulation of the networks, systems, applications, and devices in a training environment, which facilitates cyber threat awareness and skills training through education, exercises and competition (NIST, 2018).

Critical infrastructure comprises physical and information technology systems and assets that are so essential to society that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety, or any combination these factors (Alcaraz & Zeadally, 2015). The energy sector is especially critical because in addition to private individuals, virtually all industries depend on this sector to function. According to CISA (2020), the energy sector, which is the focus of this thesis, is well aware of its vulnerabilities and is leading a significant voluntary effort to increase its planning and preparedness.

During this thesis project, it was discovered that IT-professionals in the Norwegian energy sector have strong cybersecurity knowledge and skills. The primary challenge however, is the lack of cybersecurity awareness and skills by employees with non-technical roles, resulting in security incidents caused by negligence or obliviousness. Moreover, there is a disconnect between IT-employees and employees who work with operational technology (OT).

This finding was part of the motivation for creating of new training program designed for use with OT-personnel. Additionally, the client organization, NC-Spectrum, has expressed a need for a training method that utilizes cyber ranges for training employees who are not experienced with information technology or information security. The client organization is introduced in greater detail in section 3.2.1. The objective of the thesis was to examine existing frameworks and methodologies for cybersecurity preparedness training and assess their effectiveness. Furthermore, the thesis aims to discover gaps in existing frameworks and methodologies for cybersecurity training, before addressing those gaps by proposing an alternate training program. Finally, an artifact was produced in the form of a training program that is designed to be used by enterprises in the energy sector. The training program includes a cyber range and an LMS (learning management system) with training content and a quiz. Because the focus of this research has been on Norwegian energy companies, the program was assessed by creating evaluation metrics derived from interviews, the foundational security principles proposed by The Norwegian National Security Authority, and "Kraftbredskapsforskriften" (Energy Preparedness Regulation).

1.1 Research Questions

In order to address the research gap identified in this thesis, the following two research questions were posed.

- How can cyber ranges be utilized as a cybersecurity training tool for OT-employees in the energy sector?
- What limitations exist in current practical training exercises and programs related to cybersecurity preparedness in enterprises in the Norwegian energy sector?

To answer these questions, a training program called OTnetic was developed, which uses a cyber range approach with elements of gamification and simulation in order to motivate employees and create practical skills to help them combat existing and future threats. The cyber range oriented training applies a narrative story, with progressively challenging tasks. In order to ensure that tasks are completed in the correct order and to reduce the learning curve, a program simulating the commands used in the Linux based cyber range was created. This is ensure that no prior knowledge of terminal commands is required to complete the training. This project aims to understand what frameworks and types of training currently exists for OT-personnel in the Norwegian energy sector, and to provide these organizations with an effective training program in order to increase their preparedness and cybersecurity posture.

1.2 Disposition

This section introduces the remaining chapters of the thesis, and provides an overview of their contents.

Chapter 2: Theoretical Background
This chapter presents existing research, theory and literature that is relevant to, or provides background on, the research project. The method used to conduct the literature review is also presented in this chapter. The following concepts are elaborated upon in the chapter: Cyber ranges, cybersecurity training, simulation and gamification. Section 2.2 presents the literature review method and the findings from the literature.

Chapter 3: Research Approach
This chapter explains the research methodology that was used during the project. Firstly, the research approach is presented. Secondly, the research strategy is described, including the role of design science research (DSR) for empirical evaluation of the artifact. Thereafter, a description of the data collection (3.2), analysis (3.2.3), and lastly a description of the

client organization and their role in this project (3.2.1).

Chapter 4: Interview Findings
This chapter presents the interview findings from the six interviews used to elicit requirements for the artifact.

Chapter 5: The Development of the OTnetic Cyber Training Program
This chapter describes the system requirements for OTnetic (5.1), the system design including the system architecture (5.2), training content that was created for the lab experiment (5.3), various tools and frameworks used in the development of the artifact (5.4), and lastly the method for evaluating the artifact (5.6).

Chapter 6: Artifact Evaluation
This chapter presents the results from the quantitative (6.1) and the qualitative (6.2) analysis conducted after the lab experiment. Furthermore, this chapter describes the different tests that were performed and their limitations.

Chapter 7: Discussion
This chapter provides discussions and analysis of the results presented in chapter 6. Furthermore, limitations of the study are presented in section 7.1, in addition to points for further development, which are outlined in section 7.4. Lastly, we present implications for research in section 7.3.

Chapter 8: Conclusion The last chapter provides conclusions from the findings, and answers to the research questions of the thesis, as well as reflections tied to the work done in this thesis.

Chapter 2

Theoretical Background

This chapter provides an overview of prior research that is relevant for the thesis. Furthermore, a literature review has been conducted to determine the state of the art in the area of cybersecurity preparedness, which aided in the development of the OTnetic cybersecurity training program. The conclusions drawn from the literature review are presented later in this chapter. Lastly, gaps in current research are identified, and solutions to close this gap are proposed.

2.1 Background

This thesis aims to use and extend state-of-the-art approaches in cybersecurity training, cybersecurity assurance, simulation, and cyber range tools and platforms. Security practices and training has been applied within industry for many years (Evans, Maglaras, He, & Janicke, 2016). Regardless, there are still weaknesses in the cybersecurity posture of many organizations, evidenced by the ever increasing number of attacks on companies around the world. Ideally, organizations would have complete cybersecurity assurance by ensuring availability, integrity, authentication, confidentiality and non-repudiation. Moreover, measures to ensure these qualities should be able to facilitate restoration of information systems by incorporating protective, detective and reactive capabilities (Kick, 2014). As mentioned earlier however, significant gaps still exist in the security posture of many organizations. Training programs used to increase security awareness, increase compliance with security policies and technologies like cyber ranges have been used in an attempt to mitigate cyber attacks, and to train employees. Gamification has also been incorporated into tools for security training. Research shows that using game design can provide engaging cybersecurity training for a wide range of roles and skill levels (Nagarajan et al., 2012). Gamification of cybersecurity training shows great promise, and can be an effective tool in providing effective cybersecurity training (Boopathi, Sreejith, & Bithin, 2015).

Despite the fact that various solutions for cyber range training already exist, most offer a fixed number of scenarios, role or domain specific limitations, minimal automation, and often lack interaction with actual emulated cyber environments, resulting in a lack of realism (Somarakis, Smyrlis, Fysarakis, & Spanoudakis, 2019). Additionally, cyber range training has not yet been adapted to suit the needs of employees working with operational technology. This type of training is still mainly directed towards employees working with cybersecurity or information technology. As IT and OT are becoming more intertwined, caused in part by vendors increasingly transitioning to cloud-based services, operational systems are more exposed to the same attacks that threaten IT systems. Furthermore, energy companies are required to make parts of the data generated by the OT systems available to customers, making availability imperative.

Furthermore, there is an abundance of cybersecurity training tools available that aim raising awareness and improve technical skills, as mentioned in the previous section. However, these tools do not take NSM's basic security principles and "Kraftberedskapsforskriften" into account. "Kraftberedskapsforskriften" describes regulatory requirements for security in organizations working with critical infrastructure in Norway. NSM's basic security principles are a set of guidelines developed for Norwegian organizations. There is also a lack of comparison between training frameworks and exercises, making it hard to establish the efficacy and differences of different training frameworks.

Considering the lack of comparison between existing training methods and which methods are most effective, a viable solution may be to perform independent research on companies in the energy sector to determine which training methods are best suited for employees this sector. As the literature review later illustrates, a gamified approach to cybersecurity awareness and skills training may be advantageous in order to engage and motivate employees. The gap between IT and OT identified in the literature can potentially be bridged by examining them separately and comparing their commonalities and differences in order to determine their relationship. Further research should be done to determine why some employees disregard the value of cybersecurity training and the importance of their participation in protecting the organization. To further close the research gap, the training program that was made during this thesis takes the unique security situation and regulatory requirements of the energy sector into account.

Organizations in the energy sector have two main departments directly involved in technology, IT (information technology) and OT (operational technology). As identified in the interviews conducted during this research project, the differences between these departments are substantial in regards to attitudes towards security, safety, update routines etc. This is due to fundamental differences in requirements and expectations related to IT and OT systems. The interview findings show that IT-employees place greater importance on issues of information and systems security. Conversely, OT-personnel are more concerned with safety and the availability of OT systems. This finding is supported by Jaatun, Moe, and Istad (2018), who state in their report about cybersecurity in digital transformation stations that there is a challenge in the energy sector with cultural difference between IT and OT employees.

2.1.1 Current State of Cybersecurity in Critical Infrastructure Organizations

In 2014, Unisys published a report summarizing the state of cybersecurity in sectors dealing with critical infrastructure by conducting a quantitative analysis. The participants were 599 different global IT and IT security executives from 13 different countries. Most of these were highly industrialized countries in North America, Europe and Oceania. Unisys (2014) report that even though 67% of the respondents say their companies have had at least one security incident that resulted in loss of confidential information or disruption to operation over the last 12 months, few of them view security as one of their top priorities. The most ominous finding was that out of all of the participants who worked with critical infrastructure, only 43% stated that they were committed to protecting the nation's critical infrastructure. Additionally, 47% stated that the root cause of security breaches was an internal accident or a mistake (Unisys, 2014).

Unisys (2014) further reports that 70% of critical infrastructure providers across 13 countries suffered a data breach in 2013, and it was found that 54% of those breaches were a result of employee negligence. Additionally, only 6% of these companies provided cybersecurity training for all their employees. The fact that 54% of breaches are a result of negligent or oblivious insiders demonstrates the need for more cybersecurity training for all employees, especially those with limited IT knowledge. Such training may be expensive, but according to research, organizations that offer new-hire cybersecurity training report approximately 76% lower average annual losses than those that do not offer such training (PwC, 2014). Currently, cybersecurity skills training is primarily limited to employees who work with IT, while other employees are limited to awareness training consisting of campaigns, newsletters and instructor-led training. Furthermore, the training sessions provided a large amount of information in a short amount of time, leading to a passive, overwhelming, and disconnected learning experience (Adams & Makramalla, 2015). As mentioned previously, one possible solution to optimise training, engage employees and increase motivation is by incorporating gamification into training.

The Norwegian Water Resources and Energy Directorate released a report in 2017 describing the current state of cybersecurity in the Norwegian energy sector by conducting a survey. Roughly half of the participants were ICT security coordinators, while the other half consisted of managers and other employees from 88 different companies. The most frequent form of attack was phishing and attempted fraud, according to 51% of the participants (Azam, 2017). However, according to 34% of the participants, the attacks that caused the highest impact were malware attacks compromising the integrity and availability of data, such as ransomware. Over 40% of these participants did not know what caused the incident, while 35% stated that it was mainly due to human error. Both of the latter two numbers decreases drastically as the company gets bigger (Azam, 2017).

There are several threats unique to the energy sector. According to Bigham, Gamez, and Lu (2003), some of the potential malicious actions an adversary can perform inside an electric SCADA system includes changing data values, changing control signals, opening breakers, fraud and overloading. Firstly, by manipulating data readings in the SCADA system, an attacker may be able to deceive the system operators in regards to power and voltages on the grid. This can put the electricity grid into a dangerous state because operators may act on false information (Bigham et al., 2003). Furthermore, an attacker could clock control signals and issue false confirmations, causing operators to think breakers are closed when they are open, or leading them to believe that a functional transformer is malfunctioning. Additionally, if an attacker is able to overload the electricity system by switching on a large amount of devices during a period of high demand for power, they could potentially cause great damage to electrical units (Bigham et al., 2003). Lastly, smart meter data could be fraudulently manipulated by malicious customers in an effort to save money on power.

Companies in the Norwegian energy sector are subject to regulations called "kraftberedskapsforskriften", which specifies physical and IT-security requirements, as well as mandatory yearly training exercises (Azam, 2017). This regulation sets the standard for security in the Norwegian energy sector. Companies that comply with the regulation fully should in theory be well protected and prepared for cyber potential security incidents. However, some organizations in the energy sector do not comply fully with this comprehensive regulation yet. Organizations that are unsure of their current security status may use a maturity model. A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline (Curtis & Mehravari, 2015). According to Curtis and Mehravari (2015), model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline. A maturity model provides a benchmark against which organizations can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement.

In order to evaluate the cybersecurity maturity level of an organization in the energy sector, a model called the cybersecurity Capability Maturity Model(C2M2) can be used. This maturity model is specifically designed to focus on the implementation and management of IT and OT assets and their operational environment (Curtis & Mehravari, 2015). The model consists of 10 domains that are logical groupings of cybersecurity practices and four maturity levels (0-3) for each domain. The model domains align well with the CERT Resilience Management Model (CERT-RMM) (Curtis & Mehravari, 2015). The model could be useful for organizations in the energy sector as a tool to continuously assess and improve their current security maturity level. Moreover, the model will allow companies to share knowledge, best practices, and relevant references. Additionally, it can enable organizations to prioritize actions and investments in the cybersecurity domain. However, the model does not provide specific methods or measures to achieve better cybersecurity preparedness. Nor does it provide training guidelines for employees or managers. However, the model could be a useful tool in combination with proper training and implementation of specific security measures and controls.

Cybersecurity training is a crucial response to a growing number of intrusions and attacks. Despite 80% of all vulnerabilities exploited being attributed to human vulnerabilities, the focus of cybersecurity has been on technology and securing systems (Adams & Makramalla, 2015). Human vulnerabilities include negligent or oblivious insiders, misinformation and limited cybersecurity skills training, malicious insiders, and third parties who have access to an organization's network, such as consultants.

2.2 Literature Review

This section describes literature review that was conducted as part of this thesis project. The method is presented first, followed by findings and conclusions. The preferred method for this literature review was a systematic literature review (SLR).

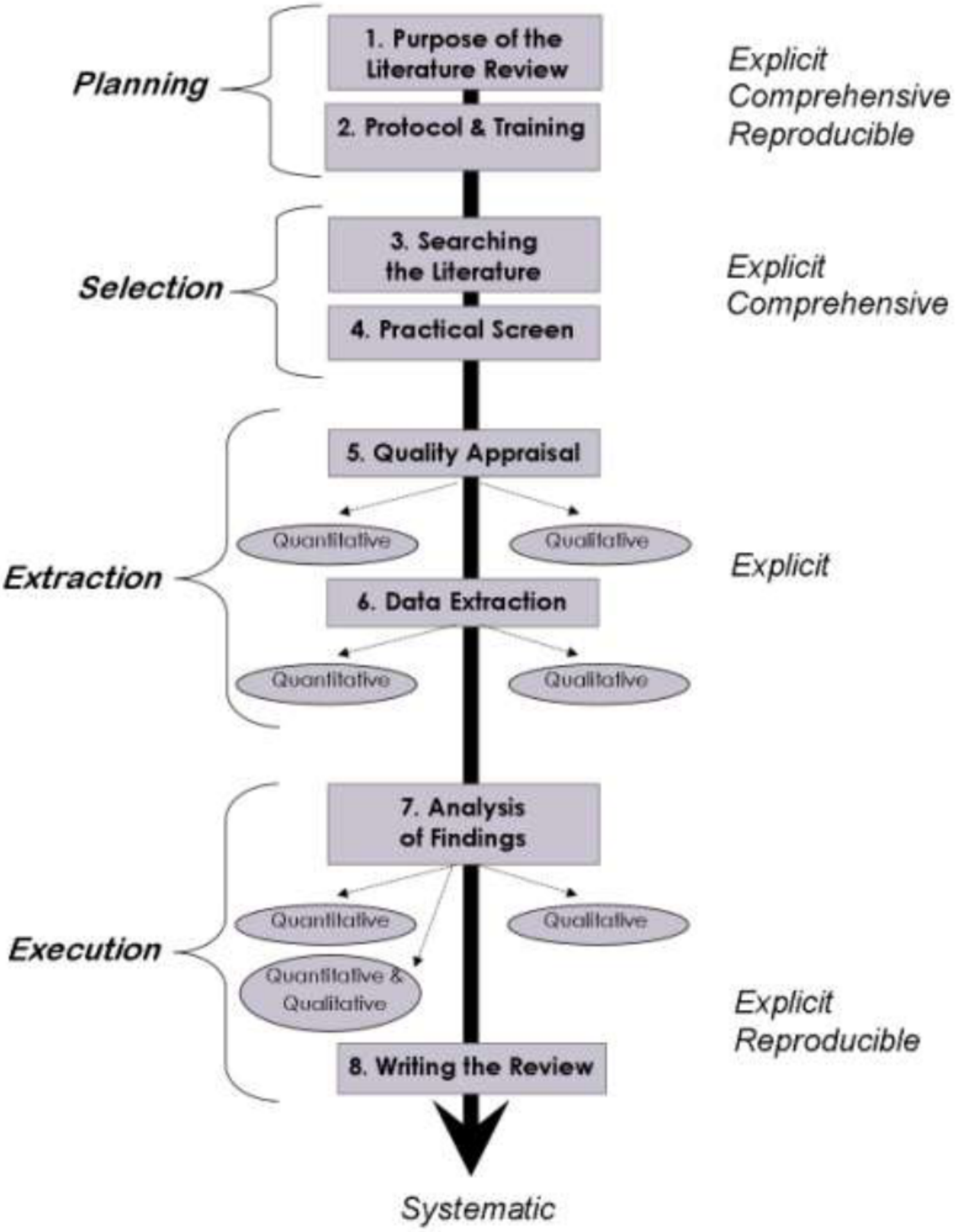


Figure 2.1: Systematic Literature Review
(Okoli & Schabram, 2010)

2.2.1 Systematic Literature Review Method

The systematic literature review performed in this thesis was performed in accordance with the process suggested by Okoli and Schabram (2010), as seen in figure 2.1. This technique integrates, evaluates and interprets findings of multiple qualitative and quantitative research studies. Literature was selected based the criteria presented in the sections below, before it was synthesized and conclusions were drawn.

Motivation

The systematic literature review provides an analytical review of literature that is relevant for this thesis project. The primary motivation for this literature review was to provide greater insight into existing training methods and programs, as well as the simulation methods and types that were available at the time of writing this thesis. This insight has established the knowledge required to propose a new training program that is better suited for companies in the energy sector, and increases training efficiency and motivation.

As this is a systematic literature review, information sources were not excluded by subjective metrics. Furthermore, literature was objectively evaluated with a focus on avoiding the interference of bias. Additionally, care was taken to not misrepresent the findings or opinions of researchers. Criteria for including and excluding literature have been carefully chosen in order to adhere to the requirements of the chosen methodology. In order to achieve the goal of understanding the literature surrounding the thesis topic better, the purpose of the literature must align with the criteria stated below.

Literature Criteria The first selection criteria was that the literature needed to align with at least one of the basic criteria defined below.

- Identify unique security and compliance requirements for organizations in the energy sector
- To classify security issues for organizations in the energy sector
- Identify and analyze existing training programs and training frameworks within cybersecurity
- Identify gaps in existing training programs and frameworks within cybersecurity
- To answer our specific research questions.

Search

The search engines and databases IEEE Xplore, Scopus and Google Scholar were used in order to search for relevant literature during the literature review process. These search engines provided sufficient results, as they aggregate literature from multiple locations and

provide a comprehensive library of sources. During the search, relevant literature was downloaded and saved in a shared folder using cloud storage software.
The following search queries were used when searching for relevant literature:

- Cybersecurity training and simulation
- Cybersecurity preparedness
- Cyber ranges
- Cybersecurity energy sector
- Energy sector security awareness
- Beredskap og sikkerhet energisektoren (Preparedness and security in the energy sector)
- Gamification of cyber training

Practical Screen

The following selection criteria were also used in the selection process.

- Publication language: The literature must be written in English or Norwegian.
- Date of publication: As the threat landscape, external compliance requirements and technology changes in a rapid pace, the literature on training for cybersecurity preparedness should have a publication date after 2010. However, if the content of the report is relevant for today, data may be extracted regardless of the publication date.
- No duplicate literature will be included.
- Literature cited by more sources will be prioritized over similar articles with fewer citations.
- Literature cited by no sources will be excluded.

Quality Appraisal

Lastly, the following criteria were set for quality appraisal of selected literature:

1. Does the literature align with the criteria for source selection as defined in the purpose section?
2. Does the study address a clearly focused question?
3. Did the study use valid methods to address this question? Does the study design and conduct try to eliminate the potential for systematic error (bias)?
4. Are the results valid and applicable to the target audience?
5. Is the literature relevant to the research questions?

Data Extraction and Synthesis of Studies

Data extraction is a systematic process where all information applicable for the research was identified and extracted from each study. The data was extracted in an external document. The extracted data was then synthesized in section 2.2.2. The extraction is not included, as it was only used as the foundation of the synthesis. The findings were summarized and the sources were linked to each other to highlight similar findings in the different studies.

Findings

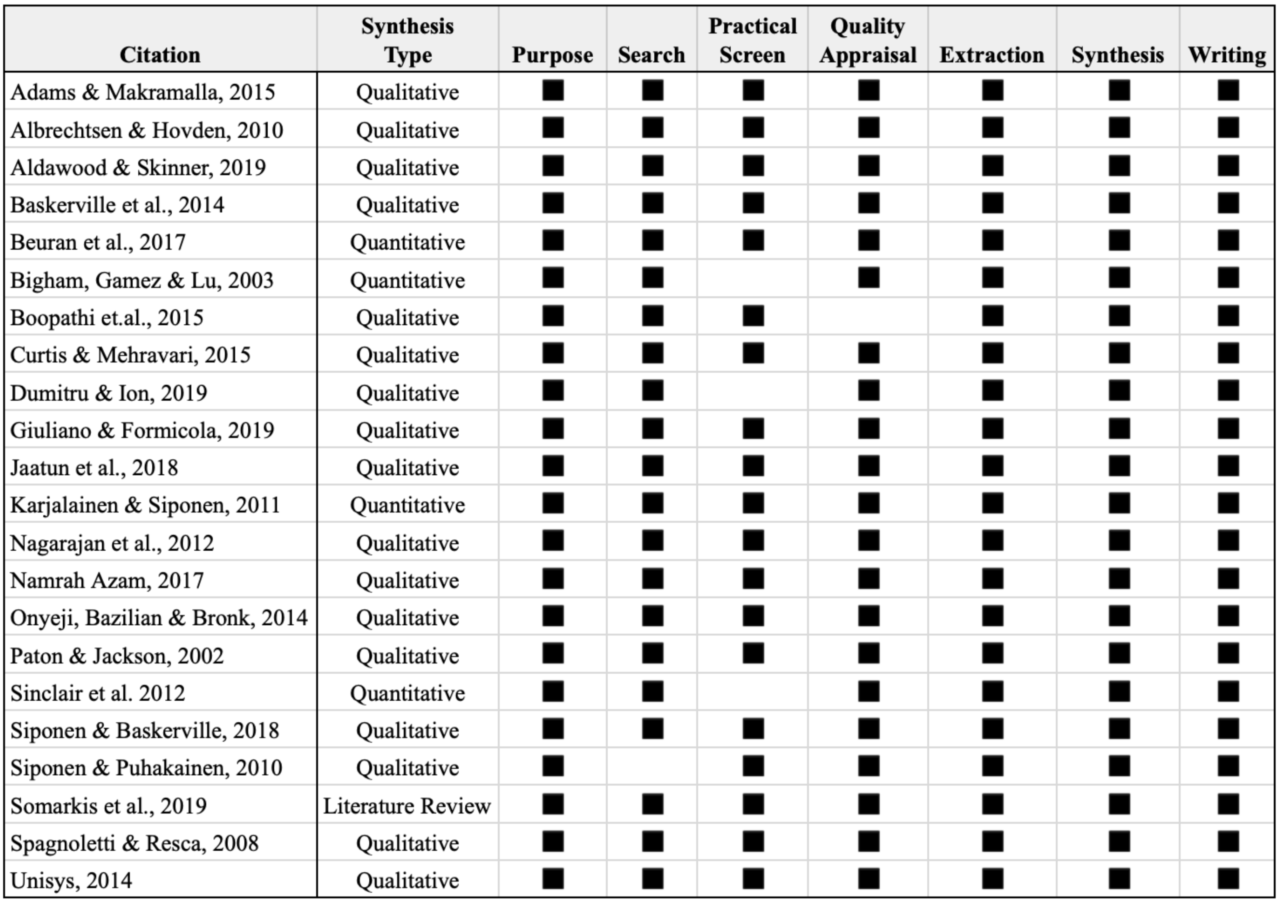
The findings in section 2.2.2 present all the findings from the synthesis. A goal for this study was to document the method of the literature review properly in order to make possible to make the findings and results reproducible. This means that if a group of researchers are following the same steps described in this report they should receive similar results.

Selected Literature

The articles listed were selected based on the inclusion criteria presented throughout section 2.2.1. Articles and studies that did not match any of the inclusion criteria, were excluded from the literature review. The following list can be used as aid to correlate the titles of selected literature with authors listed in the table below. A total of 22 articles were selected for this literature review.

- Cybersecurity skills training: an attacker-centric gamified approach (Adams & Makramalla, 2015)
- Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study (Albrechtsen & Hovden, 2010)
- Challenges of implementing training and awareness programs targeting cybersecurity social engineering (Aldawood & Skinner, 2019)
- Incident-centered information security: Managing a strategic balance between prevention and response (Baskerville, Spagnoletti, & Kim, 2014)
- Cytrone: An integrated cybersecurity training framework (Beuran et al., 2017)
- Safeguarding SCADA systems with anomaly detection (Bigham et al., 2003)
- Learning Cybersecurity Through Gamification (Boopathi et al., 2015)
- Evaluating and improving cybersecurity capabilities of the energy critical infrastructure (Curtis & Mehravari, 2015)
- Cybersecurity educational programs: costs and benefits (Dumitru & Ion, 2019)
- ICSrange: A Simulation-based Cyber Range Platform for Industrial Control Systems (Giuliano & Formicola, 2019)

- Cybersikkerhet i digitale transformatorstasjoner (Jaatun et al., 2018)
- Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches (Karjalainen & Siponen, 2011)
- Exploring game design for cybersecurity training (Nagarajan et al., 2012)
- Informasjonssikkerhetstilstanden i energiforsyningen (Azam, 2017)
- Cybersecurity and Critical Energy Infrastructure (Onyeji et al., 2014)
- Developing disaster management capability: an assessment centre approach (Paton & Jackson, 2002)
- Assessing emergency management training and exercises (Sinclair, Doyle, Johnston, & Paton, 2012)
- Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example (Siponen & Baskerville, 2018)
- Improving employees' compliance through information systems security training: an action research study (Puhakainen & Siponen, 2010)
- Model-driven cyber range training: A cybersecurity assurance perspective (Somarakis et al., 2019)
- The duality of information security management: Fighting against predictable and unpredictable threats (Spagnoletti & Resca, 2008)
- Critical Infrastructure: Security Preparedness and Maturity (Unisys, 2014)



Citation	Synthesis Type	Purpose	Search	Practical Screen	Quality Appraisal	Extraction	Synthesis	Writing
Adams & Makramalla, 2015	Qualitative	■	■	■	■	■	■	■
Albrechtsen & Hovden, 2010	Qualitative	■	■	■	■	■	■	■
Aldawood & Skinner, 2019	Qualitative	■	■	■	■	■	■	■
Baskerville et al., 2014	Qualitative	■	■	■	■	■	■	■
Beuran et al., 2017	Quantitative	■	■	■	■	■	■	■
Bigham, Gamez & Lu, 2003	Quantitative	■	■		■	■	■	■
Boopathi et.al., 2015	Qualitative	■	■	■		■	■	■
Curtis & Mehravari, 2015	Qualitative	■	■	■	■	■	■	■
Dumitru & Ion, 2019	Qualitative	■	■		■	■	■	■
Giuliano & Formicola, 2019	Qualitative	■	■	■	■	■	■	■
Jaatun et al., 2018	Qualitative	■	■	■	■	■	■	■
Karjalainen & Siponen, 2011	Quantitative	■	■	■	■	■	■	■
Nagarajan et al., 2012	Qualitative	■	■	■	■	■	■	■
Namrah Azam, 2017	Qualitative	■	■	■	■	■	■	■
Onyeji, Bazilian & Bronk, 2014	Qualitative	■	■	■	■	■	■	■
Paton & Jackson, 2002	Qualitative	■	■	■	■	■	■	■
Sinclair et al. 2012	Quantitative	■	■		■	■	■	■
Siponen & Baskerville, 2018	Qualitative	■	■	■	■	■	■	■
Siponen & Puhakainen, 2010	Qualitative	■		■	■	■	■	■
Somarkis et al., 2019	Literature Review	■	■	■	■	■	■	■
Spagnoletti & Resca, 2008	Qualitative	■	■	■	■	■	■	■
Unisys, 2014	Qualitative	■	■	■	■	■	■	■

Figure 2.2: Assessment Criteria

2.2.2 Findings from Literature Analysis

This section presents the findings elicited from the selected literature presented in figure 2.2 and section 2.2.1. As the literature covers many different aspects of cybersecurity, the findings were divided into different sections based on common themes. The following topics were selected for this literature review: use of theoretical frameworks for improved training, cybersecurity training for preparedness, simulation and gamification, and incident response.

Use of Theoretical Frameworks for Improved Training

According to Puhakainen and Siponen (2010), there is a lack of research on theory-based and empirically evaluated training programs. There are however, a number of theories that can aid in improving the learning outcome of employee training. Moreover, much of the literature on training use anecdotal conclusions. This can be avoided by using theory-based training programs, and empirical testing such as action design research (ADR) or design science research (DSR). In their ADR project, Puhakainen and Siponen (2010) were able to validate the efficacy of their training program. The program used two different learning theories as its foundation; the universal constructive instructional theory(UCIT), and the elaboration likelihood model (ELM) (Puhakainen & Siponen, 2010). Training programs and tools that lack an underlying theoretical foundation may be effective in certain scenarios, but fail to provide value in other situations due to lack of understanding of the tool's limitations (Puhakainen & Siponen, 2010). Therefore, security training programs should provide a theoretical explanation for how and why the program works. Empirical evidence further indicates the practical efficacy of the program. During the thesis project, empirical data was generated by evaluating the efficacy of the training program with appropriate participants. Participant selection is further detailed in the participant selection part of section 5.6.1.

Alternative theories that can be used in order to increase employee compliance includes punitive measures such as sanctions and other deterrence theories. Despite non-punitive measures like cognitive education and training being more effective in justifying compliance in certain types of people (Puhakainen & Siponen, 2010), Puhakainen and Siponen (2010) explain that using sanctions does diminish computer abuse. However, according to Pahnila, Siponen, and Mahmood (2007), sanctions and other negative reinforcement strategies only increase the intention to comply, not actual compliance. Conversely, training employees on safe computer use and company policies may prove more effective.

Puhakainen and Siponen (2010) break theoretical orientation of the training into three categories when theory of education is used. These are (1) behaviorism, (2) cognitivism, and (3) constructivism. The first of which emphasizes instructor-led teaching with one-way interaction, the specification of measurable and observable behavioral objectives and quantitative measurement, and the use of reinforcement to gain the learning outcomes. The latter stresses the interactive, two-way communication between the learners, which activates the learners' thinking processes and critical reflection of their knowledge (Karjalainen, 2009; Hung, 2001). One theory that can be used to design effective training includes the universal constructive instruction theory (UCIT).

The universal constructive instructional theory is a four-phase framework used to guide the training design process. The four phases are (1) determination of the instructional task, (2) diagnosis of current state of the learner, (3) constructing and delivering instruction, and (4) diagnosis of success (Puhakainen & Siponen, 2010). The learning task can be defined as the overall goal or outcome of the training, and is the sum of the learners current knowledge and required knowledge. After determining the learning task and establishing the current knowledge of the learner, instructional tasks can be constructed and delivered. Lastly, success is assessed by verifying to what degree trainees have acquired relevant knowledge. This is the process that was in the lab experiment conducted in this thesis.

One of the crucial elements for the design and delivery of instructions is functions. The functions of UCIT are related to knowledge, and are defined as: (1) acquisition of knowledge, (2) storage of knowledge, and (3) use of knowledge (Puhakainen & Siponen, 2010). The basic components of instruction are defined as the (1) learning environment (including the instruction, teaching methods and media), (2) the learning task (i.e. better cybersecurity preparedness in OT-personnel), (3) the learners, and (4) the place in which the instruction takes place (Puhakainen & Siponen, 2010). Acquisition of new knowledge (function) and the learner (component) forms the core of learning (Puhakainen & Siponen, 2010). Moreover, the training should leverage the learners previous knowledge in order to efficiently acquire new knowledge, which can be assessed via surveys or interviews. In order to effectively stimulate the learners previous knowledge prior to delivering instructional tasks, Puhakainen and Siponen (2010) suggest using group discussions with practical tasks. Furthermore, employees should be divided into different groups based on their knowledge levels. However, how predictable will these changes be? The theory described next can be used an indicator the efficiency of training.

The elaboration likelihood model (ELM) explains how predictable, long-lasting behavioral changes can be achieved through cognitive processing, and that short-lived changes can be avoided by not relying on cues. Prerequisites for cognitive processing includes motivation (Puhakainen & Siponen, 2010). Therefore, training should use learning and instructional tasks that are personally relevant for the learners. Cognitive processing of persuasive information is necessary for long-lasting behavioral changes (Puhakainen & Siponen, 2010). It is therefore important for a training program to facilitates cognitive processing. Puhakainen and Siponen (2010) further state that avoiding reliance of cues is essential, as changes relying on cues are short-lived and unpredictable. Cues include reactions of others, speaker credibility, external rewards and the attractiveness of the speaker.

Cybersecurity awareness training aims to change and develop attitudes and perceptions of employees to act more responsibly and follow the internal security policy. According to Karjalainen and Siponen (2011) this can be achieved by employing a training framework based on the understanding that the nature of information security training is persuasive and non-cognitive. They argue that IS security procedures are non-cognitive because they are created in an organizational context, and not necessarily based on scientific reasoning or facts. There are three existentialistic features of IS security training: (1) the existence of security-sensitive organizational assets, (2) threats towards these assets, (3) different social, technical and organizational mechanisms to protect the assets (Karjalainen & Siponen, 2011). Karjalainen and Siponen (2011) further state that due to the intangible nature of IS security threats and assets, the consequences of having bad information information may be difficult for employees to understand. Therefore, employees have to understand the consequences of their actions, for example the consequences of sending confidential information in plain text over an unencrypted connection. There are three different levels of thinking related to cybersecurity: meta, critical and intuitive (Karjalainen & Siponen, 2011). The meta-level is about the fundamental questions, for example "Why is cybersecurity important?". The critical-level is about critical thinking related to conventional activities, meaning that one critically reflects upon the actions being performed. Lastly, intuitive thinking refers to conventional activities in practice. A person's intuitive thinking is based on previous experiences like upbringing, education and other personal experiences. Critical thinking allows for change in the intuitive thinking (Karjalainen & Siponen, 2011).

Cybersecurity Training for Preparedness

Training and simulation in the domain of cybersecurity is already well established, with multiple training methods and simulation frameworks being proposed. This provides a lot to work with in terms of relevant research material. One the findings from the literature was that simulation exercises greatly increases the skills and motivation of employees (Paton & Jackson, 2002). According Paton and Jackson (2002), multiple simulations and exercises should be used in order to create predictive validity. Disaster readiness and planning is of great importance in the energy sector, as they are responsible for critical infrastructure. These are also situations of high pressure environments.

According to Sinclair et al. (2012), training in high pressure environments will not only allow for technical and managerial skill development but will also give an indicator of how the participants are likely to react to stressors, and what should be done in order to minimize the negative reactions to these stressors. The goal of such training is to develop a form of stress resilience and competency when new decisions have to be made in a critical emergency situation. However, opportunities for training with real world disasters are few and far between. This makes it difficult for people working with critical infrastructure to acquire realistic disaster response experience, without some form of simulation-based training.

Beuran et al. (2017) have established a set requirements for an effective cybersecurity training program. The requirements are as follows: a cybersecurity training program should (1) contain appropriate training content for the target audience in terms of knowledge and ability levels; (2) contain training content corresponding with the skills the program aims to develop; (3) use hands-on activities and exercises to make the training more memorable and realistic; (4) reach a large audience to generalize the training; (5) have sufficient cost contra performance characteristics to make the program sustainable in the long term.

Security awareness training is typically provided using top-down delivery methods, such as lectures, e-mail campaigns, leaflets and posters. Through their research however, Albrechtsen and Hovden (2010) demonstrate that local employee participation, collective reflection and group processes produce a mutual understanding of routines in organisational work, which is fundamentally important for the interaction in an organization. Interaction in groups facilitates participation and collective thinking. Additional methods to enrich the learning experience and motivate trainees further is to add gamification by applying game-design elements and game principles the training process.

Simulation and Gamification

There are several benefits to using simulation based training in the energy sector, and in the cybersecurity domain in general. Some of the benefits of simulation based training include increased self-efficacy for training subjects, increased situational awareness and development of shared mental models for the team (Paton & Jackson, 2002). Furthermore, such training exercises facilitate development of specific skills, as well as increasing the motivation of employees. By giving a team of employees a common goal to work towards, their ability to collaborate increases as well. For training exercises to be efficient, accurate and relevant feedback is important to ensure cost effectiveness and future needs. Moreover, feedback after training increases the motivation and interest of trainees, in addition to reinforcing self-efficacy (Paton & Jackson, 2002). Cybersecurity awareness training plays a key role in an organization's ability to remain prepared for future cyber attacks. Adams and Makramalla (2015) claim that typical security awareness programs do not equip employees with the necessary skills required to actively participate in cyber attack prevention. Further, they suggest that gamification of cybersecurity training is an effective way to cost-effectively arm employees with cybersecurity skills to better protect the business while reducing the financial impact of cyber attacks (Adams & Makramalla, 2015). Gamification is the process of enhancing a specific service by implementing game design elements in a non-game context. The goal is to enhance the user's overall value creation and experience (Adams & Makramalla, 2015). As mentioned previously, gamification of training exercises increases the skills and motivation of employees (Paton & Jackson, 2002).

Some crucial game design elements that are useful in cyber attack simulations are: progress mechanics, player control, problem solving and storytelling (Adams & Makramalla, 2015). Problem solving is an important element used in game design that fosters collaboration and critical thinking in order to solve problems. Moreover, the cyber-attacker community's ability to find common goals and collaborate to achieve them is illustrated to the employees, creating a better understanding. When designing games for training and educational purposes, training goals must be clearly defined (Nagarajan et al., 2012). Additionally, Adams and Makramalla (2015) suggest three relevant components that help employees stay motivated and engaged in the training exercises:

1. Feedback: Visual feedback like losing lives, triggering warning screens or earning rewards. As long as the employees are engaged in the game, the game will provides feedback, evaluate skill levels, and create obstacles to evaluate the various skill sets of the employees and comparing those results to the target level of achievement.

2. Increased challenge: Increasing difficulty is a progress mechanic used in game design. Employees require increasing difficulty in order to stay engaged, and apply critical thinking.

3. Opportunities for mastery: The game should provide opportunities to develop skills and excel, granting a feeling of mastery and increased confidence.

Boopathi et al. (2015) suggest a gamified CTF-style learning approach as a tool for teaching cybersecurity. The competition or training session would consist of three rounds. The first round is a learning round where participants are given tutorials related to cybersecurity concepts like binary exploitation, reverse engineering, forensics, web application security etc. This round engages the participants and ensures that they are familiar with basic security concepts and implications. Next is the Jeopardy round. This is the round in which knowledge regarding previously introduced concepts are tested by solving problems and questions of varying complexity. Last is the interactive round, which aims to apply the concepts of cybersecurity in real world scenarios (Boopathi et al., 2015).

In their game, the researchers have four levels. The first level tests general programming skills, the second level tests web application security concepts, the third level tests application security concepts. Lastly, reverse engineering and forensics concepts are tested (Boopathi et al., 2015). The testers provided the participants with a virtual machine containing applications with known vulnerabilities that when exploited, would produce a flag. The game could be performed in a cyber range style, with two teams aiming to gather points by both attacking the other team, and defending their own team's machines. Boopathi et al. (2015) concur with Adams and Makramalla (2015) that utilizing gamification in training makes the learning experience more fun for participants, increases motivation, and produces a greater learning outcome.

According to Giuliano and Formicola (2019), cyber ranges can be employed for team building, cyber training, capture the flag (CTF), research and development, testing, assessment, and recruitment. Furthermore they have found that maintenance staff of Industrial Control Systems (ICS) are generally not aware about information technologies, and even less about cybersecurity problems, which supports the need for additional training in the energy sector (Giuliano & Formicola, 2019). Cyber ranges offer this opportunity, but current research is lacking cost-effective solutions verticalized for the industrial domain (Giuliano & Formicola, 2019). Furthermore, Spagnoletti and Resca (2008) have identified that new and emerging threats necessitates the ability to develop a formative context where learning and innovation are favoured over risk evaluation and action plans in order to establish a more secure environment in organizations.

Incident Response

Regarding emergency management and emergency operations centers (EOCs), little information exists about training assessment. Moreover, accepted preparedness practices are often based on anecdotes, which are generally lacking in systemic study and objective validation (Sinclair et al., 2012). This is largely due to difficulties associated with measuring team performance and training effectiveness. However, organizations using training and assessment programs often have programs unique to their organization, and the monitoring and the evaluation aspect of the training is often overlooked. Therefore, it is mostly unknown how effective emergency training is. The study conducted by Sinclair et al. (2012) concludes that given the complexity of disaster response environments, training should be based on correspondingly comprehensive techniques to provide holistic training and evaluation. Sinclair et al. (2012) further argue that even though such training is more expensive, the benefits of further developing capabilities for unknown events and disasters will lower the risk of losing lives in the event of an actual disaster.

In relation to emergency response training it is recommended to divide the feedback session into two different debriefs, an informal hot debrief immediately after the exercise, and a more formal cold debrief held about a month after the exercise (Sinclair et al., 2012). Cybersecurity awareness training as of today mostly comes in the form of lectures or seminars held by security professionals. The target audience are often a group consisting of employees with different backgrounds, ranging from managers to IT professionals to employees from the finance department to name a few. It is difficult to create appropriate content that is understandable for participants with different backgrounds. Furthermore, seminars often lack engagement from the participants, where there is mostly one-way communication, making the training less memorable in contrast to hands-on activities like case studies or other more practical exercises (Nagarajan et al., 2012).

According to Baskerville et al. (2014), incident-centered information security management is a theoretical and practical framework consisting of three elements: (1) situational analysis, planning, and operation in the prevention paradigm; (2) situational analysis, planning, and operation in the response paradigm; and (3) close attention to the time continuum in deciding the balance of effort between (1) and (2). Both prevention and response are important paradigms, but focus can shifted between them as organizational needs change. Unsophisticated and repetitive attacks may only require prevention, but as the sophistication of attack increase, so must the emphasis on activities in the response paradigm (Baskerville et al., 2014). Typically, organizations that focus more on incident response operate in unstable security environments, while ones that operate in a stable security environment focus more on prevention.

2.2.3 Conclusions from the Literature Analysis

With the continuously evolving sophistication and increasing frequency of cyber attacks, organizations face both a set of predictable threats and a set of new and emerging problems. There are a plethora of methods for reducing risk of cyber incidents through implementation of pertinent technical and procedural countermeasures. However, such techniques are more effective on repetitive and simple attacks. Advanced attacks, in addition to attacks that exploit the vulnerability of the organization's human resources, are harder to prevent with technical countermeasures. For example, despite most mature and developed organizations having technical countermeasures against phishing attacks in place, such attacks are still remarkably prevalent.

Organizations would be wise not to rely solely on their IT-department as protection against the aforementioned attacks. Involving all employees by facilitating the acquisition of cybersecurity skills across the entire organization will greatly increase their capability in the preventive paradigm. Furthermore, research shows that traditional security awareness training is ineffective. Such training typically focuses on educating employees about common cyber attacks, and providing a limited set of best practices for fundamental security. Training in this fashion may help raise awareness around security issues, but lacks the practical and reflective aspect of security skills training that would help protect the organization from future attacks. A contributing factor to the inefficiency of regular awareness training is its failure to engage and motivate employees. Research shows that attack simulations and practical security skills training is significantly more beneficial.

Firstly, simulations allow employees to train for events and incidents that have rare occurrences. Secondly, simulations increase motivation among participants, increase memory retention, create skills applicable in real incidents, and foster collaboration by providing common goals. These factors ultimately culminate in a greater learning outcome for employees. Finally, the benefit of aforementioned training methods are enhanced by the implementation of gamification, which increases motivation and gives the participants a feeling of mastery.

Gamification has been shown to further increase the positive benefits provided by cybersecurity simulation training. Game design elements such as visual feedback, practical tasks and progression of difficulty aid in the development of critical thinking and problem solving, which would help to prevent unfamiliar threats. Very few organizations currently provide cybersecurity training to all employees, suffering greater annual financial losses as a result. In Norway, organizations in the energy sector are required by law to follow a set procedures and requirements that relate to cybersecurity. Moreover, the law demands yearly training exercises to be performed. Compliance with this regulation has not been determined in this literature review, as there is little research on the legal compliance of Norwegian companies in the energy sector.

Despite the large amount research on the aforementioned topics, there still exists a gap in the research, which will be addressed in this thesis. Firstly, there is very little research on area that focuses on Norwegian companies. Secondly, there is lack of studies directly comparing and testing the efficacy of cyber range training against current common training methods, such as lectures. Lastly, the studies on cyber ranges as training tools mostly focus on training IT security professionals in penetration testing and defense. Moreover, there is a lack of research on how these tools can be applied to training for OT-personnel and other groups outside of IT professionals.

In summary, organizations in the energy sector should provide cybersecurity awareness and skills training for all employees. Many companies in the energy sector have small IT-departments, with few cybersecurity professionals, resulting in a general lack of resources when identifying and mitigating attacks caused by both external attackers and negligent insiders. Furthermore, over 50% of breaches in critical infrastructure organizations are a result of employee negligence. Therefore, training is a crucial investment to protect the enterprise and reduce financial losses resulting from successful cyber attacks. Lastly, simulations and game design elements should be included in the training. A maturity model can be used in order to assess their current level of cybersecurity preparedness, and determine measures for how to improve the security posture of the organization.

Chapter 3

Research Approach

A research strategy describes the plan of the research project. For this project, the research strategy is based on the activities included in the design science research method (DSR). DSR has gained more popularity over the last years, especially for research related to information systems (Cater-Steel, Toleman, & Rajaeian, 2019; Thuan, Drechsler, & Antunes, 2019). The activities shown in section 3.1 are specifically tied to design science research (DSR) topics related to the development and improvement of information systems (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007).

3.1 Design Science Research

For this thesis the design science research approach was employed, where an artifact is designed and produced as a result of the research project. This method was chosen because it facilitates the creation of an end product, or artifact, that is useful and provides a benefit to the industry. Furthermore, this approach focuses on the design and development of artifacts and performance evaluation of such artifacts. DSR aims to solve problems by developing an artifact that solves problems identified in the real world and evaluating it against alternative solutions. The objective of this thesis project was to develop a cyber security training program for OT-personnel in the Norwegian energy sector, called OTnetic. As the objective of DSR aligns well with the objective of our project, this approach was found to be the most appropriate.

In DSR, both qualitative and quantitative research methods are used in the process of creating and evaluating the artifact. First, a qualitative approach is used in order to lay the foundation for the requirement analysis. Second, a quantitative approach is used to evaluate the artifact based on metrics elicited from the requirement analysis. The goal is to provide a useful contribution to IT-professionals in the Norwegian energy sector. Interviews were conducted in the beginning of this project, in order to provide better insight regarding the status of cybersecurity preparedness in the Norwegian energy sector, regulatory requirements, and what type of training program would be most valuable for Norwegian energy companies. The following principles were employed, which are based on the design science research methodology described by Peffers et al. (2007), for designing and developing the artifact:

1. Activity 1: Problem identification and motivation
   Establish the research problem and justify the need and value of a solution. A useful tactic to achieve this is breaking up the problem conceptually to understand the degree of complexity in addition to the scope of the problem. This activity is described in chapter 1.

2. Activity 2: Define the objectives for a solution
   Define the objectives of a solution based on the problem definition. It is important to emphasize that these objectives should be both possible and feasible. The objectives, or requirements, are elicited from interviews, which is described further in chapter 4.

3. Activity 3: Design and development
   This activity is where the artifact itself is designed and created. The artifact can be any designed object, but it must include a research contribution which is embedded in the design of the artifact itself. Examples of artifacts are models, methods and constructs. The main objectives for this activity is determining the functionality as well as the architecture of the artifact about to be created. This activity is described in chapter 5.

4. Activity 4: Demonstration
   Use the artifact in a demonstration where the objective is to solve one or more instances of the problem. This demonstration could be in the form of experimentation, simulation or case study. A requirement for this activity is to include effective knowledge of how the artifact should be used to solve the problem. The results from the demonstration of the artifact is presented in chapter 6.

5. Activity 5: Evaluation
   Evaluate the demonstration(s) and analyse whether the artifact supports an effective solution to the research problem. This activity requires knowledge about what metrics to use when evaluating the artifact based on what problem it should solve. The evaluation should provide empirical evidence from the demonstration(s). The evaluation of the artifact, based on the results from the lab experiment, is described in chapter 7.

6. Activity 6: Communication
   Convey the problem and if it is important, in addition to the degree of importance and why. This activity is mainly about communicating to other researcher (as well as other relevant audiences) why this artifact is effective at solving the problem in question. This activity was performed after finalizing the thesis. The findings were presented to NC-Spectrum, with a focus on further development and how the artifact

can be integrated with current cyber training in the energy sector.

Firstly, interviews were conducted with people who work in the energy sector. Secondly, interview data was analyzed. The findings are presented as user stories in appendix E. These findings were then used to elicit requirements for the artifact, and user stories were produced based on the requirements. The user stories are categorized into two parts, (1) software requirements, and (2) training content requirements. The testing and evaluation of the OTnetic training program consisted of a lab experiment and a questionnaire as part of the evaluation stage, which revealed how effective the artifact is in terms the participants' ability to acquire new knowledge.

3.2 Interviews

As mentioned previously, a qualitative method was applied in order to provide insight when eliciting requirements for evaluation of the produced artifact. Qualitative methods are applied in the early stages of the design science research process, as they lay the foundation for the requirement analysis (Hevner & Chatterjee, 2010). For the qualitative part of this project, interviewing was used as the primary data collection method.

In total, six interviews were conducted; four of the interviews were conducted with four different Norwegian energy companies, and two of them were conducted with companies who respond to security incidents in the energy sector. The interviews were semi-structured, and two interview guides were created to prepare and structure different focus areas with questions relevant for requirement elicitation. The primary focus areas were the enterprise's current status on cybersecurity training, attitudes towards cybersecurity, and the participants' opinions on using cyber range training with practical challenges to learn more about cybersecurity. The interviews were conducted remotely, using Microsoft Teams. This method was preferred due to the different geographical locations of the interview subjects, and COVID-19 considerations. Each interview lasted approximately one hour. All but one interview were recorded and subsequently transcribed. The one interview that was not recorded, by request of the interview subject, was performed by writing notes instead. After transcription, every interview was analyzed and broken down into themes, and the data was used to elicit requirements for the artifact. All interview recordings and transcriptions were deleted after use out of respect for the privacy of the interview subjects.

3.2.1 Client Organization

The client organization for the thesis project is called NC-Spectrum. NC-Spectrum is a Norwegian company with high competence in networks and information security. Their mission is to develop, sell, deliver and operate competence and services in the domains of digital infrastructure and information security (NC-Spectrum, n.d.). NC-Spectrum has participated actively during the project by offering their advice and aiding in selecting interview subjects.

Frequent meetings have been held with the client organization to keep stakeholders up to date on the progress of the project.

3.2.2 Selecting Appropriate Interview Subjects

Prior to development of the thesis, NC-Spectrum expressed the need for a training program tailored for OT-personnel, as the they work with multiple energy companies and has identified a need for additional training. Moreover, NC-Spectrum requested that a cyber range was to be part of the program. Because the project aims to determine if cyber range training can be more effective than traditional training methods for OT-personnel in the energy sector, employees working with OT in Norwegian energy companies would be most suited to provide the appropriate answers to establish the requirements for the artifact, in addition to the client organization of this thesis project. Fortunately, as NC-Spectrum works with security incidents in the energy sector, they were able to provide valuable insight related to the unique security challenges that OT-personnel face. This should provide an additional layer of reliability regarding the training content and the requirements elicited from the interviews, as OT-personnel may not be sufficiently informed about previous breaches and how they themselves were involved either directly or indirectly.

OT-personnel is an umbrella term covering different professions working with operational technology, which is operation of physical processes and machinery and software used to carry them out (i.e. SCADA software). The artifact that was produced is intended for operations engineers with knowledge of how to implement, operate and maintain operations systems in an energy company. Employees working with this type of technology do not share the same skills, attitudes and knowledge of cyber security as employees working with information technology (IT).

3.2.3 Qualitative Analysis

As the research method chosen for the thesis was DSR, the interviews were used to provide requirements for the artifact based on what the interview subjects want and expect from the training program. Additionally, the interviews provided a number of themes that describe the common denominators related to cybersecurity preparedness in the energy sector. The data used to construct the requirements were a combination of the data elicited from these interviews (both from questions and themes), and the data provided by the existing literature and theory.

After the interviews were conducted, they were transcribed in order to maintain the underlying meaning and context. Furthermore, transcription simplified the analysis process, as it provided a searchable and readable representation of the interviews. The answers were then summarized in the findings section, and later compared to existing theory from the literature review, to check for correlations and validity. Lastly, the requirements were elicited from the findings. The interview guides used during the six interviews are included in appendix A and B.

Chapter 4

Interview Findings

This chapter outlines the interview findings used for requirements elicitation for the OTnetic cyber training program. The interview guides are located in appendix A and appendix B. System requirements were derived from six interviews, which were conducted in order to understand how cybersecurity training with OT employees in the energy sector is performed. Additionally, it was desirable to understand and how this training can be improved to increase the security preparedness and awareness in the sector. Four of the interviews were conducted with employees from companies that work in the energy sector, and two interview was with a security company that has energy companies as customers. Evaluation metrics for the artifact are described in section 5.6.3.

All of the interview subjects work with operational technology (OT) directly, indirectly as managers of OT-personnel, or by having energy companies as clients. The primary function of the interviews was to gain insight into the status of cybersecurity training in the Norwegian energy sector, and uncover potential weaknesses in current training methods. Additionally, the interviews provided information about what types of alternative training methods may be more suitable than what is currently provided, and how cybersecurity training can be improved. All the findings have been grouped into four different themes.

4.1 Training in the Energy Sector

OT-personnel in the Norwegian energy sector are given minimal amounts of training in regard to cybersecurity concepts and best practices. Most of the training they receive relates to health and safety, as well as training from vendors on how to use the equipment they provide. Additionally, some security training is provided in the form of video lectures and classes. However, the concepts that are described, which mostly relate to phishing, are simple and lack any element of practical problem solving or critical thinking. All of the companies interviewed have security policies that they are required to read. They are also required to sign an agreement stating that they have understood its contents.

However, these policies are typically reviewed once a year at most, and compliance with the policies varies depending on the individual employee. Several interview subjects informed us that policy compliance is sometimes overlooked when it prevents them from performing their duties efficiently. One of the interview subjects mentioned that they have requested more in-depth and challenging training, as much of the teaching material is currently simple and intuitive for most trainees. Some interview subjects stated that in current training programs, much emphasis is placed on confirming email legitimacy with the IT department, and not sharing passwords and user accounts with coworkers. Furthermore, internal IT employees are tasked with holding information meetings when the company has experienced a cyber attack, but it is unclear if any proactive solutions are discussed. Another interview subject mentioned that the company has organized multiple security campaigns. These include mandatory lectures with questionnaires that ensure participant engagement. It is unclear what happens if an employee does not successfully get through the course, but this would be followed up by management. These campaigns also provide employees with the opportunity to raise questions and receive additional information and clarification if they are interested. None of the companies interviewed had security training directed specifically at OT-personnel, and when asked, most of them expressed that they would like more thorough training with practical and gamified elements. Overall, most companies in the energy sector have security policies related to privacy, password complexity and expiration, and use of multi factor authentication. Additionally, basic training is provided in attempt to prevent phishing attempts, which most of the interview subjects report as effective.

Two of the interview subjects stated that attack simulations are used in training. In this case, simulations refer to lectures including explanations of how attacks are performed. Such lectures are usually followed by reflective exercises like answering questions related to the given lecture. Although such exercises may help improve the security awareness in the organization, there is great potential for improvement of exercise efficiency in terms of employee motivation and engagement, and subsequently increasing the learning outcome. Moreover, most scenarios created for cybersecurity training focus on phishing attacks. However, if the organization is to be truly prepared, widening the surface in terms of attack types is imperative. One of the energy production companies that was interviewed has an ICT-handbook containing policies on cybersecurity procedures and incident response plans in addition to descriptions of previous attacks and how they were mitigated. The handbook is used when the organization experiences new attacks that require action to be taken, not as a training aid. This handbook could be a useful implementation that could be part of a training framework for the company and other organizations working with critical infrastructure, as it would create a shared knowledge base for companies with similar security environments.

Preventive security measures are considered most effective, because small and medium sized companies lack the capacity to identify and detect and mitigate attacks in real time. The focus has instead been on streamlining services and optimize cost efficiency; little attention has been directed towards modernizing. On the other side, security awareness is viewed as an essential element to strengthen the first line of defense. Greater security awareness among employees would likely increase the organization's detective capabilities, as employees with higher awareness of the current threat landscape are better suited to detect cyber attacks such as phishing. Employees are less susceptible to phishing if they are aware of the consequences and able to identify certain attributes exposing the attack. Furthermore, employees being unaware of the notion that phishing is a form of fraud, can make them feel powerless and incapable. Medium sized companies have small IT departments with no or few employees with background in cybersecurity. These department are too small and lack of resources results in poor detective controls. A limited understanding of information security makes it difficult to establish a strong security culture as employees do not have sufficient knowledge about IT and information security. However, several companies are tackling this problem by hiring younger employees, and performing annual security awareness training followed by a quiz to evaluate effectiveness. Other companies have decided to outsource their cybersecurity responsibilities to other Norwegian or foreign companies, making it difficult to determine how well the information is processed and secured.

Additionally, these companies have little or no idea about the internal security in the companies they outsource their security to. As mentioned previously, Norway has strict regulations for organizations responsible for critical infrastructure. Be that as it may, it is highly difficult to be entirely compliant with these regulations, especially for smaller companies that have few IT employees and small security budgets. For instance, organizations in the energy sector are required to have specific roles and responsibilities designated in order to respond to incidents and perform disaster recovery. In addition to the legal requirements placed upon these organizations, many of them follow self imposed regulations by attempting to comply with guidelines provided by the Norwegian National Security Authority (NSM). Despite their efforts, compliance is an ongoing project that may never be fully realized for some. Although the security is not yet at the level many companies would like, security agencies such as NSM and PST are quick to respond and assist these companies when they are attacked, due to the crucial role they play in the protection of society. The energy companies also face some unique challenges in regards to security that other organizations with operational technology are not subject to. Contrary to other companies with OT-systems, energy companies are required to share information produced by the OT-systems with the general public. This means that companies in the energy sector cannot always use air-gapping to prevent unauthorized communication with OT-systems, creating additional security implications.

The quality of cybersecurity training in the energy sector has improved in recent years. This can in part be attributed to NorSIS, who have been providing new training content as well as the organizing a national security month each October. However, one of the interview subjects states that even though the training has become more interesting in general, the participants' interest in cybersecurity is still low. The quality of the training could be improved by giving the participants a better understanding of what cybersecurity is, and the potential impact weak security has on the company, or society. Furthermore, the training should be divided into different specific topics that highlight important aspects of cybersecurity before introducing the participants to cyber range training. The cyber range should mainly focus on the blue team training as this should help participants know when and how to react to a certain threat. Moreover, this could also help participants know who they should alert about a discovered threat. Lastly, there is a need for increased frequency of training. Some companies only remind their employees of security issues after an attempted attack. This is helpful when a new attack type or angle is discovered, but a more proactive approach may be beneficial.

All interview subjects stated that the training they received was relevant and depicted an accurate portrayal of the security issues they face. One subject mentioned that the training content provided by external security consultants and The Norwegian Center for Information Security is encouraging, but the national security month can be overly technical. Furthermore, although most of the training content itself is adequate, poor delivery of the material can make the training uninteresting for some participants. By providing a cyber range platform which gamifies aspects of the training, the motivation to participate in training will likely increase. Moreover, many employees expect the systems and networks they use to be resilient to external threats, and view security as the IT department's responsibility. One interview subject informed us about the importance of penetration testing as a useful tool to raise awareness illustrating the importance of security to management. When asked about the relevance of their training programs, one subject stated that there needs to be a basic understanding of the security principles before training, which suggests that some of the training does not take the employees' previous knowledge into account. This is a missed opportunity as employees with greater IT knowledge could be provided with more advanced training, and vice versa. Furthermore, some IT departments are understaffed, resulting in a decreased focus on security. It was mentioned that employees get most of their information about security incidents from the media, and that the IT department shields their employees from the impact of incidents, as not to worry the employees. However, ensuring that employees are aware the potential impact of cyber threats will improve their desire to adhere to better security practices. It is clear from the interviews that low frequency of training is an issue that could prevent many organizations from responding appropriately to new and evolving cyber threats.

Lastly, the interview subjects were asked to elaborate on what they and their organization would like the training program to include. Answers included the importance of security routines and policies, scenario training with practical tasks, compliance with kraftberedskapsforskriften, the importance of access control, security in engineering stations, and asset management for industrial control systems. Moreover, training scenarios could include what one would see and be exposed to if attacked, how to mitigate the attack, and who to alert. This would allow participants to inform management about relevant security measures. Furthermore, participants could receive training related to the importance of changing default usernames and passwords, and how to propose appropriate security requirements to vendors. Lastly, it was suggested that the training program should implement security concepts and skills that are applicable in a personal setting, as well at work. Participants should be taught the importance of strong security, and connect personal security measures to how this impacts the company they work for, as this would make it more motivating to attend training sessions.

When asked about the desire to use a training program with practical tasks in a cyber range environment, all interview subjects responded positively. They mention that the idea sounds like it would be fun and exiting, while simultaneously creating a better understanding security issues. One interview subject informed us that they have requested more practical training, specifically using scenarios in order to train and prepare for potential future attacks. The utility and effectiveness of the training would rely however, on how well it is delivered. The security concepts would have to be explained well and given proper context before any practical training can take place. According to one of the interview subjects, the combination of theory, relevance and context of the security concepts, in conjunction with the practical aspects of using the information, is what will make the training program more useful than alternative solutions. This would increase knowledge retention and allow participants to see the relevance and context of their training. Furthermore, showing participants how easily security vulnerabilities can be exploited will help them gain a greater understanding of the potential impact of poor security habits.

4.2 Compliance with Security Policies

There are several reasons why compliance with internal security policies could differ. For instance, difference in company size and experiences with previous data breaches could affect the policies. Three of the subjects mentioned that it is difficult to make employees follow instructions written in the policy. Applying technical security controls such as forcing employees to change passwords after a given period of time were more effective than written policies alone. One of the security issues addressed in the interviews, is that employees have left sensitive information in their working environment (i.e. home directory or desktop). The first issue with this is that sensitive information should not be located anywhere else than in the database it is intended to be in, according to the policy of this informants company. The subject believes the cause of this is related to a more general problem, which is that cybersecurity often is viewed as an obstacle for productivity.

The second issue, which the subject addresses as a much more difficult issue to tackle, is that employees do not clean up after themselves in the virtual domain. The subject informed us that it should not be any more difficult to clean up after themselves in the virtual world when it is expected that is done in the physical world (i.e. cleaning your desk). The interview subject further states that productivity is viewed as more important than security for the average employee. For example, an employee may download an application they need without asking the IT department, if they are in a hurry. However, another interview subject stated the opposite, specifically that employees are generally compliant with the internal security policy, and that employees are asked to read through and understand the policy and confirm this with a signature. The conclusion is therefore that internal security policies are followed to a lesser extent if they affect productivity negatively, suggesting a lack of motivation to follow them. There is also a general lack of focus on enforcing the policies. Lastly, one subject stated that there are no policies preventing use of personal devices on the company network. This is not uncommon, but there are inherent security issues, such as the risk of malware spreading from personal devices to the company's network and their devices (Miller, Voas, & Hurlburt, 2012).

All interview subjects stated that they had internal procedures and policies regarding cybersecurity. Examples include acceptable use policies, requirements for multi-factor authentication, and privacy policies. Additionally, there are several system integrated security policies, such as password change each month or each quarter. However, three of the participants stated that these policies are often only brought up during the on-boarding phase when hiring new employees, and are not repeated and enforced as often as they should. Only one of the participants stated that it is not mandatory to sign and agreement with these policies.

4.3 Cybersecurity as a Shared Responsibility

Three of the interview subjects agreed when asked about the notion that there is a dichotomy between OT and IT employees in terms of what security aspects they deem most important. All the interview subjects agree that OT employees place greater importance on health and safety, as well as availability of systems. On the contrary, IT employees are more invested in the confidentiality and integrity of systems. Furthermore, many employees who work with OT systems expressed that the rules and guidelines put in place by the IT department in order to secure the company and its infrastructure are working against the productivity goals of OT employees. The OT employees' primary concern is their ability to access the systems they need for their duties without being hindered in the process. Password policies and access control that is built into these systems are disliked by some employees, although they understand the importance of such protection measures. Ironically, some employees who work with SCADA systems express that they would feel safer using a shared user account, as mistakes made in the system would be harder to attribute to a specific user when using a shared user account. One of the companies interviewed has employed people that work with both OT and IT. In this organization, the IT department seems to have a greater understanding of both sides, as there is a better bridge of communication between the two.

Overall, the divide between OT and IT has diminished over the last few years however, as IT employees are given more responsibility and insight into the OT world and vice versa. However, there is still a distinct difference between the two in terms of their work tasks and responsibilities. OT employees work directly with the systems, and are responsible for personnel safety, whereas IT employees are responsible for the general security of architecture, systems and information.

The degree to which employees feel that security is a shared responsibility varies from company to company, and person to person. Many employees view security as the IT department's responsibility, and feel that security measures are an annoyance that often hinders productivity. To ensure that all employees are aware that security is a common responsibility, a campaign was started by one of the companies which was directed at managers in order to teach them that they are responsible for the security of the organization, which was not entirely clear previously. Furthermore, when asked if they would know how to help secure the company, and if security measures should be implemented, the response was that security measures are important and necessary to secure the organization, despite their hectic work days. Again, it was stated by one interview subject that the IT department protects other employees from security incidents. They expressed that this could reduce stress among the employees, but that it also leads to relaxed attitudes regarding security issues.

Mixed responses were received when interview subjects were asked whether or not OT employees posses the necessary skills and knowledge required in order to actively participate in the protection of the organization. Some interview subjects expressed that employees did possess security skills, and provided an example where a phishing attack was discovered and thwarted. Furthermore, employees are taught to ask the IT department if they have any doubts regarding the legitimacy of emails. Another interview subject concurs with this assessment, and states that employees are given extensive information about phishing, which is a threat they have become much better at protecting against. However, most other threats are unlikely to be detected by OT employees. Anomalies in SCADA for instance, are very common, and employees are able to detect them by themselves, but are not equipped with the skills to asses whether the anomaly is a caused by an error, or an external threat. They are not used to considering the possibility that an external actor wants to harm the system.

4.4 Cybersecurity Awareness and Experiences with Cyber Attacks

During the interviews, subjects were also asked what the most critical security threat would be to operational technology, what attacks would have the greatest impact, and what attacks occur most frequently. The responses ranged from phishing and ransomware, to hacking and intrusion of critical infrastructure, and abuse of SCADA systems. Phishing occurs most frequently, along with ransomware, which are demanding to handle and has great potential for damage and financial losses. Furthermore, a hacker abusing SCADA systems could potentially cause power outages in thousands of homes and businesses. Additionally, loss of customer information and documentation of assets and systems would be critical incidents.

Three of the interview subjects stated that employees who work with OT are aware that there can be vulnerabilities present in the systems, but they were not worried about the reality of them being exploited by a threat actor. However, one subject stated that it is unlikely that employees are aware of vulnerabilities in OT-systems, as people who use SCADA do not worry about the possibility of the system being hacked. When asked about vulnerabilities in SCADA systems that have been discovered and/or patched, this interview subject mentioned an attack against a Florida water treatment facility where hackers used TeamViewer to access the internet facing SCADA system, which did not have a firewall and was protected only with a password used by other systems at the facility. Another subject informed us that these systems are scanned regularly, and that vulnerabilities are discovered occasionally. Some of the vulnerabilities are inconsequential, while others require immediate attention. The company has service level agreements with vendors stating that the vendor is responsible for notifying the company when a vulnerability in their product is discovered. When it comes to SCADA systems, this is strictly enforced. However, when it comes to power stations and programmable logical controllers (PLC) this might be less consistent, as these systems rarely change or get updated. However, new facilities are to a larger extent designed and built with security in mind, and importance is placed on patching and continuous updating of software.

All of the subjects have witnessed an incident caused by a cyber attack in the company their working in at some point. Two of the companies have fallen victim to crypto-malware, but the impact of each attack was vastly different. The third experienced a breach of computers which resulted in servers being established on their infrastructure. The last interview subject had not witnessed any major events, but had experienced one machine being infected with malware. The impact of each attack was very different. In general, mitigation methods that were used included formatting computers and restoring from backup, segmenting the network, and removing malware from infected computers and servers. Furthermore, network based intrusion detection systems (IDS) were implemented in order to prevent future attacks. Most of the attacks mentioned by interview subjects can be prevented by employees using computers and software responsibly and securely at work. Thus, it is likely that such attacks could be prevented by raising the security awareness and developing the practical security skills of employees. Based on the responses from interview subjects, it is reasonable to suggest that phishing attacks leading to crypto-malware infections are the most frequently attempted and successful attack, as well as the one with the greatest impact on the organization financially. Prevention of ransomware infection can be greatly improved by increasing the employee's ability to detect and report phishing attempts.

Two of the subjects state that cybersecurity can be challenging for OT-personnel to comprehend, especially the terminology and IT as an infrastructure. One of the subjects further states that he suspects this is because employees view IT as a tool-set to complete their work, and to be used for social media and entertainment in their spare time. In essence, they have little interest for how information technology works, and do not want to spend energy on it in their daily lives. One of the subjects states that cybersecurity is only perceived as difficult and perplexing if it interferes with their work or halts productivity. The problem with terminology is a more generic problem related to general lack of interest when it comes to learning subject concepts used in other sectors or domains. However, another subject stated that cybersecurity is not perplexing and most of them know how information security works and are aware of security issues. Despite this, the subject proceeded to explain that few employees have in-depth knowledge of how cybersecurity works and how significant the consequences can be if a major cyber incident occurs. All of the interview subjects were positive to a new and more practical training program, and argued that it could be beneficial with training is able to concretize different topics within cybersecurity and visually represent how a cyber attack can unfold, and what the possible consequences of the attack are. One of the subjects thinks that this could make employees understand how certain restrictions could prevent a potential data breach. Moreover, training frequency should increase, and it would be beneficial to include scenarios in the training where incidents are categorized, and participants are allowed to respond according to their internal guidelines.

4.5 Conclusion

Overall, findings from the interviews with Norwegian energy production companies suggest that cyber security is regarded as an important focus area in the industry. Strict governmental regulation and highly competent support systems provide energy companies in Norway with the knowledge and skills needed to protect our critical infrastructure. Additionally, most companies in the sector aim to follow NSM's basic security principles, which are comprehensive and cover aspects ranging from identification of threats and vulnerabilities, to preventive, detective and mitigative measures. However, many organizations are not fully compliant with regulations or NSM's guidelines. Due to the complexity of these instructions and the resource constraints in small companies, complete compliance is an ongoing project. Furthermore, cybersecurity training is not always prioritized, despite yearly training being specified in the regulation. Current training methods typically focus on lectures, with predefined questions used to test the employees' knowledge after training. This form of training is less effective than simulations or other practical training methods, as it is less engaging and motivating for participants than practical tasks and simulation exercises.

During the interviews, it became apparent that a more practical and interactive approach to training is necessary in order to motivate participants, resulting in improved learning outcome. Furthermore, since the target audience of the training has limited information security knowledge, basic security principles should be prioritized first. Moreover, it would be beneficial to provide the ability to increase training frequency. This is all possible by using a cyber range where participants are given information and practical tasks. The inclusion of gamification in the form of storytelling with progression and feedback, increasing difficulty and a scoring system.

In conclusion, Norwegian energy companies have solid and comprehensive guidelines for how to improve and maintain a strong cybersecurity posture. However, lack of time, financial resources, IT-personnel and practical training necessitates improvement in regards to cybersecurity preparedness. This can be achieved by creating and implementing a training program with the purpose of raising cybersecurity awareness and practical skills, with a focus on actively participating in the protection of the organization by being able to identify and mitigate recurring threats. Additional training would help these companies be better prepared for future cyber attacks. By utilizing a cyber range as a platform for employees to perform practical tasks presented in a story, participants will be more motivated to complete training, gain a greater understanding of security issues, and have the ability to increase frequency of training.

Chapter 5

The Development of the OTnetic Cyber Training Program

This section describes the design and development of the OTnetic cyber training program. Furthermore, the tools and programs used to create OTnetic are described. OTnetic was developed using multiple open source programs and tools, and consists of three major parts: (1) a learning management system with training activities, (2) a customizable cyber range with multiple virtual machines, and (3) a python program containing the narrative story with practical challenges and a scoring system with flags.

5.1 System Requirements

This subsection describes what requirements were elicited from the interview findings and literature review, and how they were selected. Several user stories have been created that can be found in appendix E. These are divided into two categories: (1) software and (2) training content.

The requirements have been sorted and prioritized using the MoSCoW prioritization model based on what the interview subjects and the client organization viewed as important. Each user story describes one requirement for the software or training content, which together form the OTnetic training program. For example, user story E.3 states: "As a moderator/instructor, I want to be able to customize the cyber range according to the users' needs, so that the training is targeted against the appropriate audience". As shown in figure 5.1, the trainee can use any computer with web browser to access the entire training program and cyber range remotely.

5.2 System Design

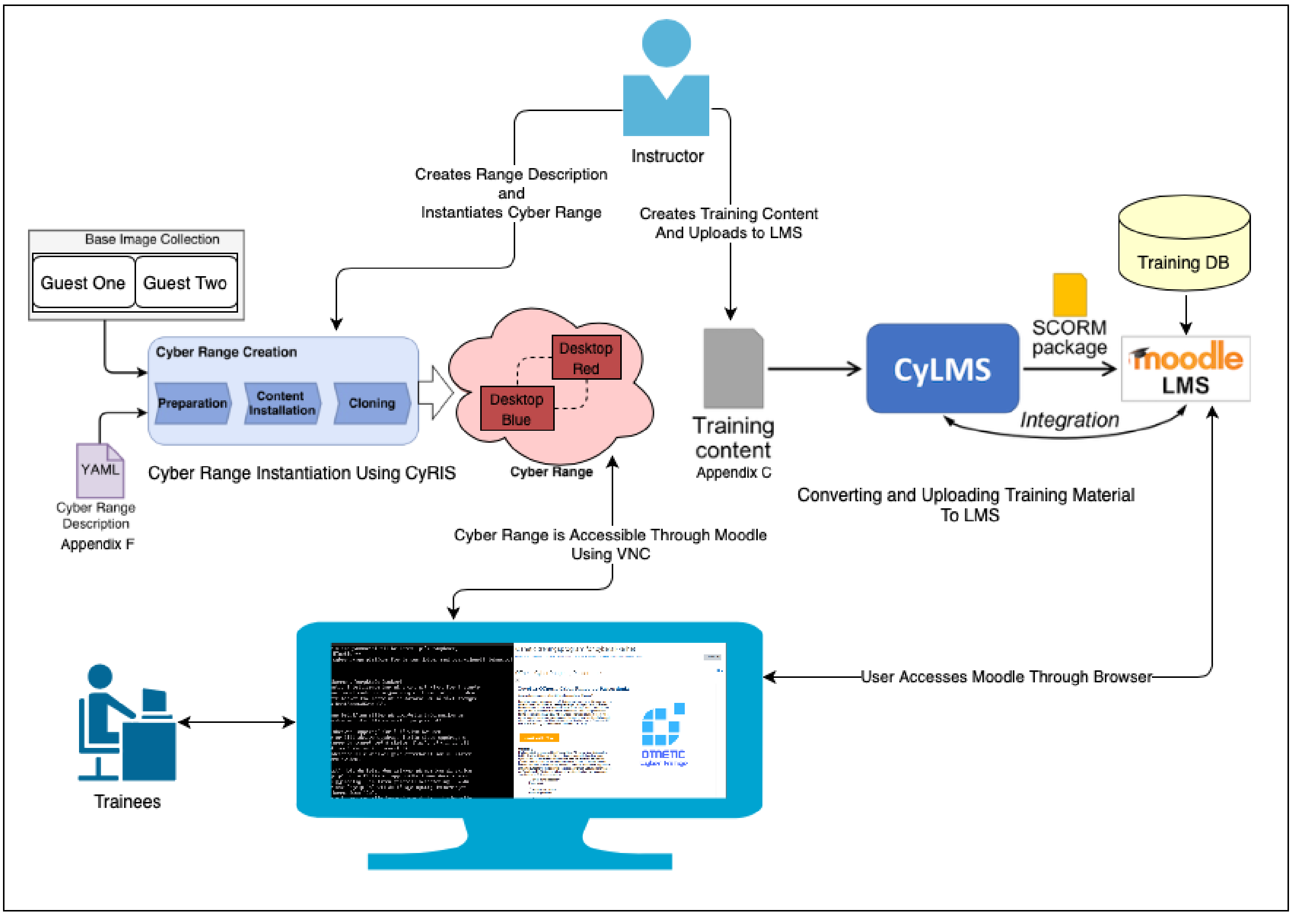


Figure 5.1: System Architecture for the OTnetic Training Program

The OTnetic system was designed using components from multiple open-source projects, which are described in greater detail in section 5.4. Firstly, CyTrONE was used to install necessary dependencies, download the virtual machine images, and set up a virtual machine with an Apache server where Moodle was installed. Secondly, CyLMS is used to convert the training content from the YAML file in appendix C to a SCORM package, which is then uploaded to Moodle. This training content was created based on the requirements from section 5.1 and user stories in appendix E. Then, a cyber range based on the description file in appendix F is instantiated using CyRIS. Lastly, a VNC connection to the cyber range was created so the participants could access the range through the training activity in Moodle. All the user has to do to use the system is access the URL that points to the Moodle server. From the LMS, they are able to perform the quiz and access the cyber range through their browser, without the need for additional software.

5.3 Training Content

The training content was developed in accordance with NSM's recommendations for digital security, as compliance with NSM's guidelines was one of the requirements elicited from the interviews, described in user story E.21. In the training program, two of NSM's web pages were used as information sources. The first article is called "Råd og anbefalinger om passord" ("Advice and recommendations for passwords") (NSM, 2019), and the other is called "Passordanbefalinger fra Nasjonal Sikkerhetsmyndighet" ("Password reccomendations from the Norwegian National Security Authority") (NSM, 2018). Furthermore, external services were used to allow the user to explore password security. One of these services is called "Have I been pwned?". This service allows users to type in their e-mail address or password to see if the address or password has appeared in a data breach. In the OTnetic training content, the service was used to check an example e-mail that has appeared in several breaches. In the pre-recorded lecture, the website was shown on screen, with the same example e-mail address. Additionally, two services called passord.net, and security.org were used. Passord.net is a Norwegian web page where users can generate strong passwords in the form of password phrases (Passord.net, 2021). The website was used as hint in one of the quiz questions in the OTnetic training program, for users who were unfamiliar with the concept of password phrases. Lastly, a service on security.org called "how secure is my password" was used. This service allows users to input a password to see how long it would take to crack it (Security.org, 2021). Most of the additional training content was developed based on the researchers knowledge of cyber security.

5.4 Tools and Frameworks

5.4.1 CyTrONE

CyTrONE is an open source integrated cyber security training project created by researches at the Japan Advanced Institute of Science and Technology (JAIST) (Beuran et al., 2017). The training framework is designed to simplify the cyber range setup process. For this thesis project, CyTrONE was installed using an installation script available on GitHub. The script, which can be found in appendix D, automatically installs necessary dependencies such as various Linux packages, pulls the CyRIS and CyLMS GitHub repositories, and downloads a virtual machine image (CentOS 7) used by Moodle and the cyber range. Furthermore, the script configures the Moodle virtual machine and generates SSH keys, as well creating a virtual machine with Moodle and Apache installed.

5.4.2 CyLMS

CyLMS was used to convert OTnetic's cyber security training content to a SCORM package, which was uploaded to the learning management system (LMS) Moodle. SCORM, which is an acronym for Sharable Content Object Reference Model, is widely used in learning management systems and e-learning platforms. The CyLMS script takes a training content file made in the YAML format, and a configuration file as the input, and creates a zip-file with the SCORM package. Furthermore, the script can be used to set up VNC access to the cyber range. If VNC is enabled, the script will automatically add a button in the training activity which opens a tab with a window into the cyber range virtual machine. This functionality facilitates OTnetic's cyber training approach, which is to let users perform practical tasks in the cyber range while simultaneously receiving information and answering related questions in the quiz accessible through Moodle.

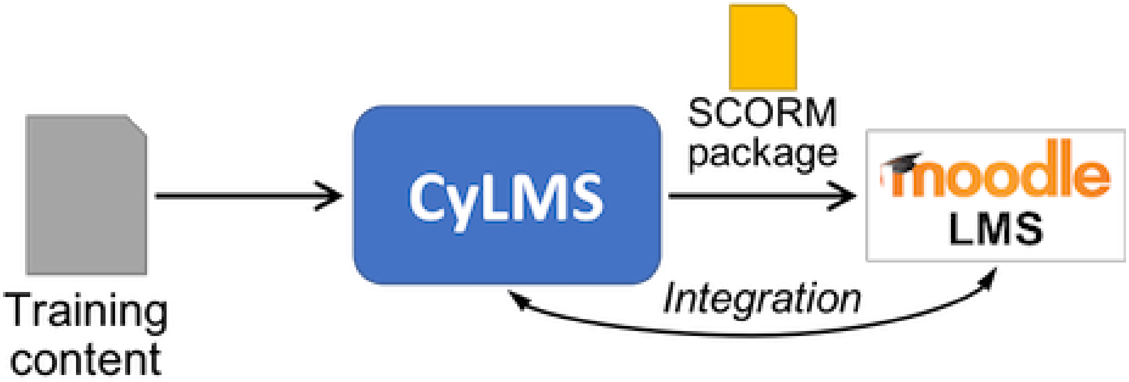


Figure 5.2: CyLMS Training Content Conversion
(Beuran et al., 2017)

In order to convert a YAML file with training content to SCORM and upload it to the LMS, the following command and arguments can be used, where "1" refers to the activity ID. The configuration file contains the IP address of the Moodle VM, the Moodle content repository, and the CyRIS cyber range directory.

```
$ ./cylms.py --convert-content training_content.yml --config-file
config_file.txt --add-to-lms 1
```

To remove a training activity, this command can be executed.

```
$ ./cylms.py --config-file config_file --remove-from-lms 1,ID
```

5.4.3 Moodle

Moodle is a free and open-source LMS used to manage user accounts and host training content. Moodle allows for the creation of a large number of users, and the administrator is able to enroll one or more users in any number of activities. Moreover, Moodle provides the ability to save grades for users based on their performance on completed training activities, and issue badges upon completion of courses or individual training activities. For the purposes testing OTnetic as an alternative to traditional cyber security training, one module was created, with a focus on password use. The training content, which is written in a YAML format, is provided in appendix C.

5.4.4 CyRIS

CyRIS is the part of CyTrONE that is responsible for cyber range instantiation.

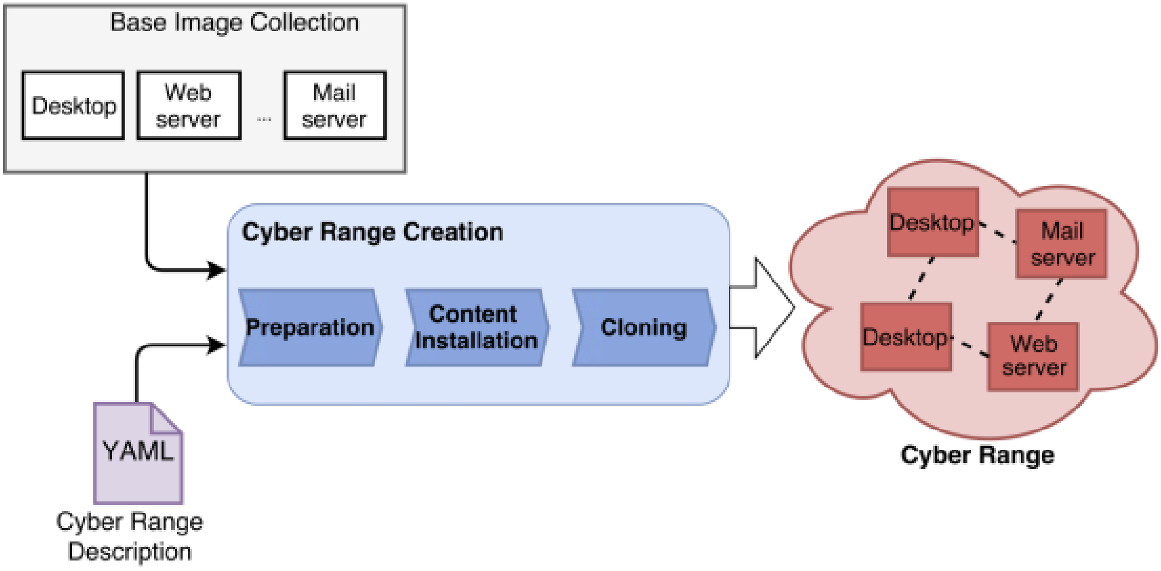


Figure 5.3: CyRIS Cyber Range Instantiation Tool
(Beuran et al., 2017)

The code in appendix F was used as a template to provide details for the cyber range instantiation. The template, written in YAML format, can easily be modified in order to change the configuration of the cyber range. In the example from appendix F, two guest machines are created. Both virtual machines are connected to the same network, so they are able to communicate with each other. Because the narrative story and simplified command line requires python3 to run on the cyber range, the instantiation template specifies that python3 should be downloaded and installed with yum onto the virtual machine called "red", during cyber range creation.

By utilizing CyRIS, cyber ranges can easily be created and destroyed with a few simple terminal commands. Firstly, to create a cyber range with the YAML file in appendix F, the following command can be run from the cyris folder:

```
main/cyris.py examples/template.yml config_file
```

To destroy the range, the following command is used:

```
main/range_cleanup.sh path_to_range config_file
```

5.4.5 noVNC

noVNC is a HTML VNC client that enables access to a remote computer through the web browser without additional softwaare installed. OTnetic uses noVNC to provide trainees with a window into the cyber range virtual machines.

noVNC requires WebSockets support, and noVNC's sister project websockify was used to fulfill this requirement.
The VNC client was run with the following command in order to enable HTTPS.

```
./utils/launch.sh --ssl-only --cert self.pem
```

The SSL certificate referenced in the above command was generated with this command.

```
openssl req -new -x509 -days 365 -nodes -out self.pem -keyout self.pem
```

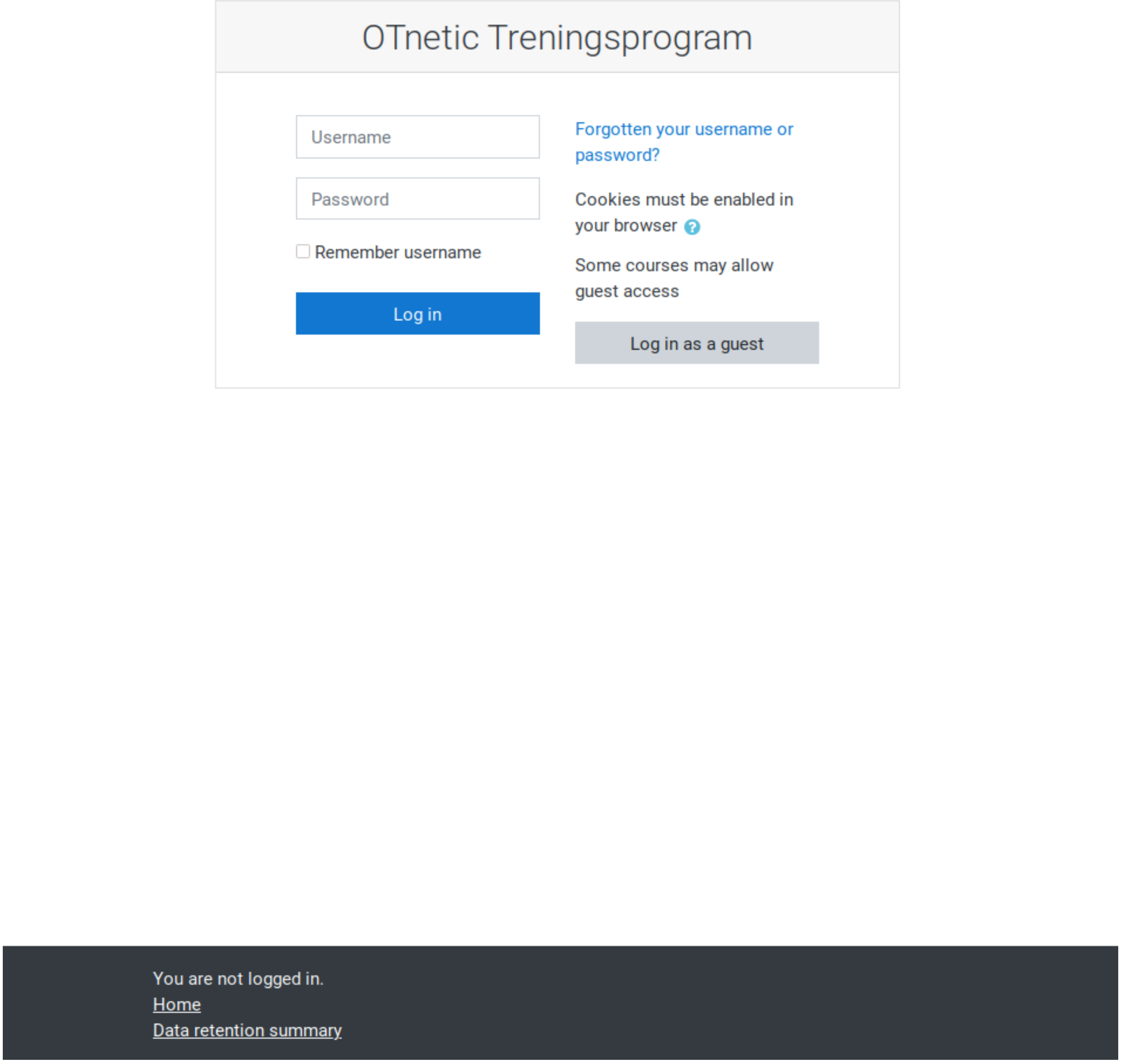
5.4.6 Apache Guacamole

Apache Guacamole is an open-source, clientless remote desktop gateway that support VNC, RDP and SSH (Apache Software Foundation, 2021). Guacamole allows users to access a server through their web browser, without plugins or client software. Initially, OTnetic used Apache Guacamole for testing purposes. The program was implemented so that external users could access OTnetic. However, during development, the Apache server on the Moodle virtual machine was made accessible via the internet and connected to a domain name owned by one of the authors of the thesis. This was done to prevent an additional layer of authentication for the end-users of the training program.

5.4.7 Training Progression

When a user is ready to start the OTnetic cyber security training program, they will open their web browser and navigate to the Moodle server's IP address. For the purposes of testing, the lab experiment instructions provided participants with a link to one of our personal domains, which forwarded the participant to the Moodle server's IP address. This was done for convenience, as a domain name is less intimidating for normal users to interact with than an IP address and port. When navigating to the correct URL, the user will be presented with the following login page.

After the user has logged in successfully, they are taken to the "activities" page. Where they can choose to enter the activity for OTnetic's password module. As the user in figure 5.5 has administrative privileges, they are also able to delete their own attempts. However, this does not apply to normal users.



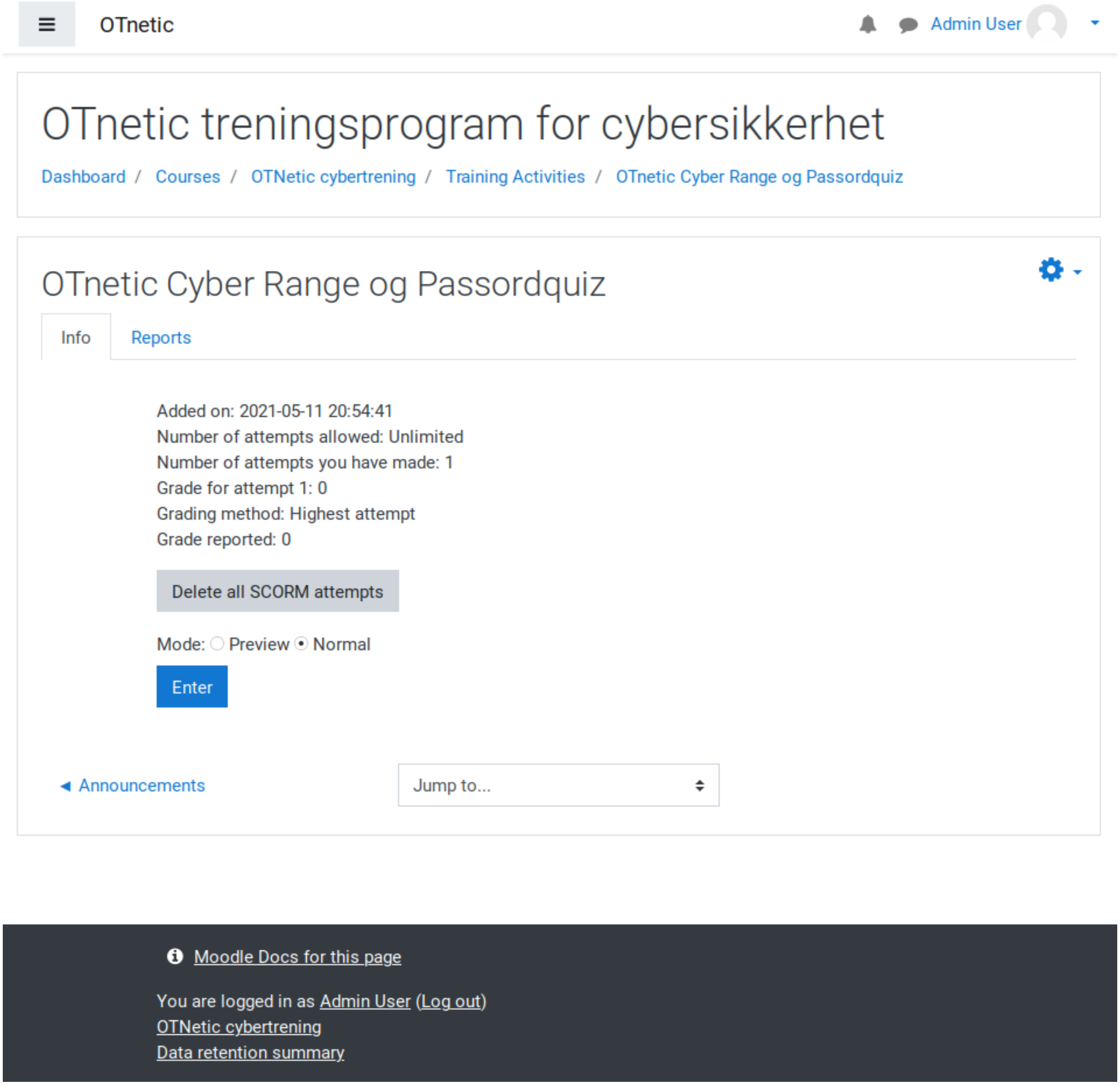
OTnetic Treningsprogram

Cookies must be enabled in your browser ?

Some courses may allow guest access

You are not logged in.

Figure 5.4: OTnetic Login Page



OTnetic

Admin User

OTnetic treningsprogram for cybersikkerhet

Dashboard / Courses / OTNetic cybertrening / Training Activities / OTnetic Cyber Range og Passordquiz

OTnetic Cyber Range og Passordquiz

Added on: 2021-05-11 20:54:41
Number of attempts allowed: Unlimited
Number of attempts you have made: 1
Grade for attempt 1: 0
Grading method: Highest attempt
Grade reported: 0

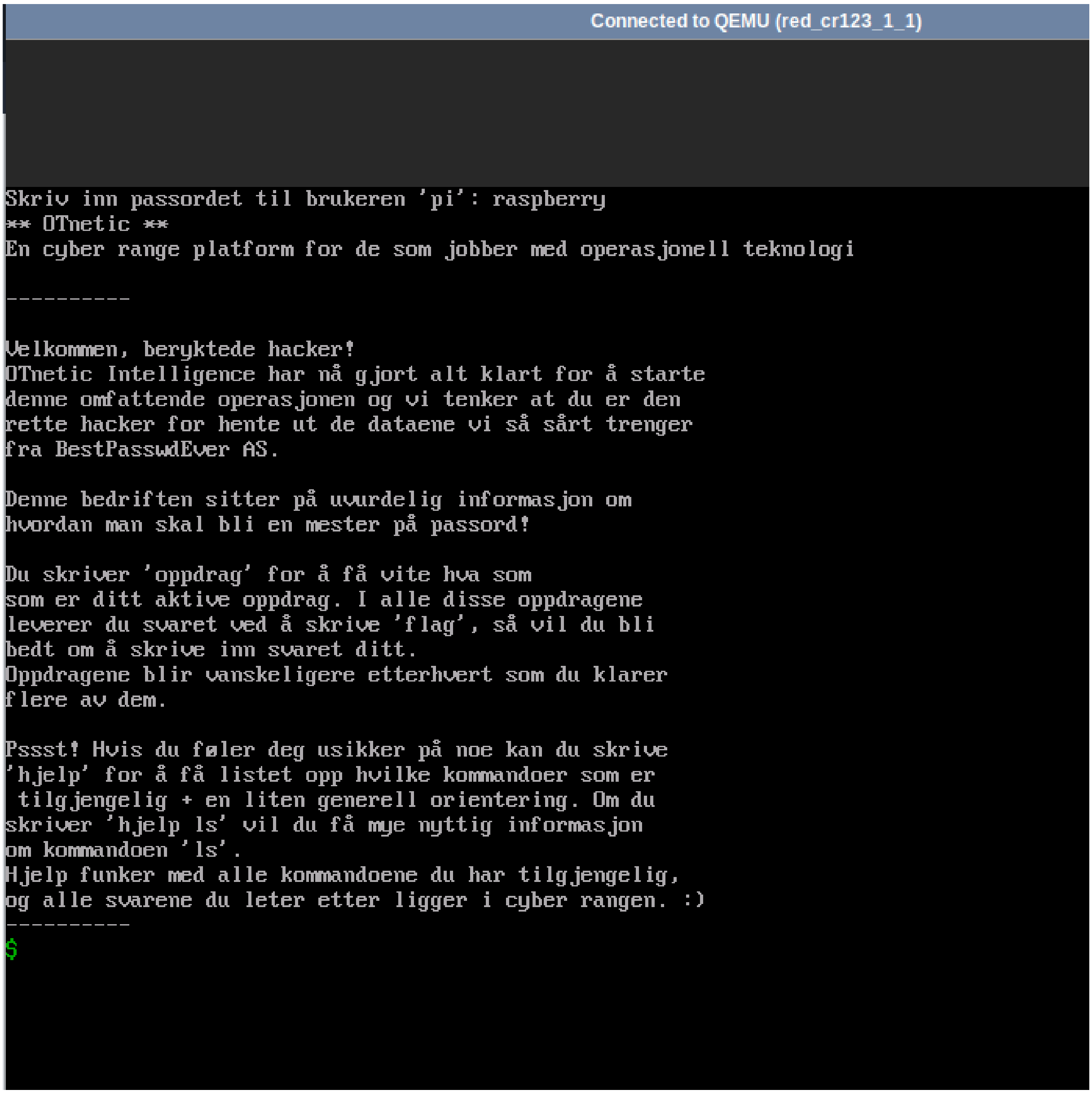
Mode: ○ Preview ● Normal

Moodle Docs for this page

You are logged in as Admin User (Log out)
OTNetic cybertrening
Data retention summary

Figure 5.5: OTnetic Activities Page

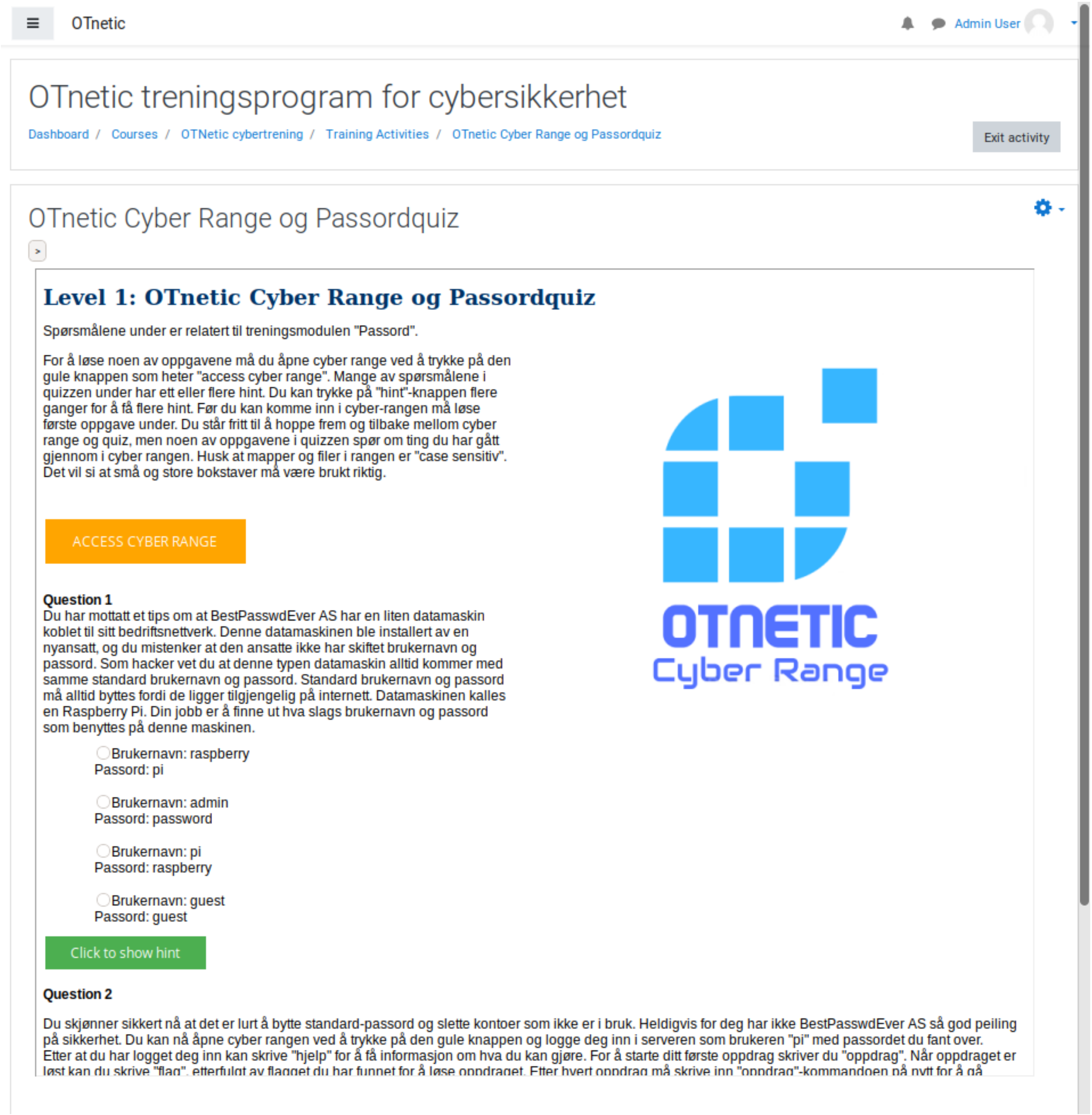
After entering the activity, the user receives information and is able to submit answers in the quiz illustrated in figure 5.7. In the quiz, there is a yellow button that can be used to access the cyber range. Access to the cyber range is provided using the VNC protocol. The user can complete practical challenges in the cyber range while answering quiz questions in Moodle. For each challenge in the cyber range, there is an accompanying "flag". Flags are used as a scoring system, and delivering a correct flag sets the current challenge as completed. The user receives a point for each flag that is delivered. The cyber range and the LMS are tightly connected, and some quiz questions will require that the user completes certain cyber range challenges in order to answer the quiz question correctly. Next, once the user has completed all the challenges in the cyber range, they can type "exit" to quit the Python program and end the module. If the user has not yet finished the quiz, they may continue.



```
Skriv inn passordet til brukeren 'pi': raspberry
** OTnetic **
En cyber range platform for de som jobber med operasjonell teknologi

----------

Velkommen, beryktede hacker!
OTnetic Intelligence har nå gjort alt klart for å starte
denne omfattende operasjonen og vi tenker at du er den
rette hacker for hente ut de dataene vi så sårt trenger
fra BestPasswdEver AS.

Denne bedriften sitter på uvurdelig informasjon om
hvordan man skal bli en mester på passord!

Du skriver 'oppdrag' for å få vite hva som
som er ditt aktive oppdrag. I alle disse oppdragene
leverer du svaret ved å skrive 'flag', så vil du bli
bedt om å skrive inn svaret ditt.
Oppdragene blir vanskeligere etterhvert som du klarer
flere av dem.

Pssst! Hvis du føler deg usikker på noe kan du skrive
'hjelp' for å få listet opp hvilke kommandoer som er
 tilgjengelig + en liten generell orientering. Om du
skriver 'hjelp ls' vil du få mye nyttig informasjon
om kommandoen 'ls'.
Hjelp funker med alle kommandoene du har tilgjengelig,
og alle svarene du leter etter ligger i cyber rangen. :)
----------
$
```

Figure 5.6: OTnetic Cyber Range

Finally, when the quiz is completed, the user can submit their answers and click the "exit activity" button to display and save their results. All progress is saved to a file when the user submits a flag, so if the user exits the cyber range before finishing all the challenges, they may restart without losing their progress.


OTnetic
Admin User
Dashboard / Courses / OTNetic cybertrening / Training Activities / OTnetic Cyber Range og Passordquiz
Exit activity
ACCESS CYBER RANGE
OTNETIC
Cyber Range
Click to show hint

OTnetic treningsprogram for cybersikkerhet

OTnetic Cyber Range og Passordquiz

Level 1: OTnetic Cyber Range og Passordquiz

Spørsmålene under er relatert til treningsmodulen "Passord".

For å løse noen av oppgavene må du åpne cyber range ved å trykke på den gule knappen som heter "access cyber range". Mange av spørsmålene i quizzen under har ett eller flere hint. Du kan trykke på "hint"-knappen flere ganger for å få flere hint. Før du kan komme inn i cyber-rangen må løse første oppgave under. Du står fritt til å hoppe frem og tilbake mellom cyber range og quiz, men noen av oppgavene i quizzen spør om ting du har gått gjennom i cyber rangen. Husk at mapper og filer i rangen er "case sensitiv". Det vil si at små og store bokstaver må være brukt riktig.

Question 1
Du har mottatt et tips om at BestPasswdEver AS har en liten datamaskin koblet til sitt bedriftsnettverk. Denne datamaskinen ble installert av en nyansatt, og du mistenker at den ansatte ikke har skiftet brukernavn og passord. Som hacker vet du at denne typen datamaskin alltid kommer med samme standard brukernavn og passord. Standard brukernavn og passord må alltid byttes fordi de ligger tilgjengelig på internett. Datamaskinen kalles en Raspberry Pi. Din jobb er å finne ut hva slags brukernavn og passord som benyttes på denne maskinen.

○ Brukernavn: raspberry
Passord: pi

○ Brukernavn: admin
Passord: password

○ Brukernavn: pi
Passord: raspberry

○ Brukernavn: guest
Passord: guest

Question 2

Du skjønner sikkert nå at det er lurt å bytte standard-passord og slette kontoer som ikke er i bruk. Heldigvis for deg har ikke BestPasswdEver AS så god peiling på sikkerhet. Du kan nå åpne cyber rangen ved å trykke på den gule knappen og logge deg inn i serveren som brukeren "pi" med passordet du fant over. Etter at du har logget deg inn kan skrive "hjelp" for å få informasjon om hva du kan gjøre. For å starte ditt første oppdrag skriver du "oppdrag". Når oppdraget er løst kan du skrive "flag", etterfulgt av flagget du har funnet for å løse oppdraget. Etter hvert oppdrag må skrive inn "oppdrag"-kommandoen på nytt for å gå

Figure 5.7: OTnetic Cybersecurity Quiz

5.4.8 KYPO

KYPO is an open source framework for hosting and managing a cyber range platform in a cloud environment. KYPO is dependent on several OpenStack services to manage the infrastructure that allows for an interactive cyber range environment.

The main reason for considering KYPO as our solution for providing the training content was the possibility to create, customize and simulate an entire infrastructure. Furthermore, OpenStack provides a graphical user interface for managing different parts of the cyber range such as virtual networks, machines instances, routers, users, etc. However, during the project it was discovered that configuring all of the required OpenStack services to make the KYPO framework work was too time and resource consuming. Furthermore, at the time of writing this thesis, neither of the authors had sufficient experience with this open source cloud framework.

5.4.9 AWS Cyber Range

The AWS cyber range is another open source project providing a bootstrap framework for creating a cyber range using the Amazon Web Services Cloud. The AWS Cyber Range project requires an AWS account, and use of the required services and resources in AWS does cost money. The AWS Cyber Range was considered as a possible solution to use for implementation OTnetic. However, the framework is made primarily for penetration testing practice, and it was considered less suitable for the types of challenges and tasks that are given to the target training participants for this project. Moreover, it was preferential to use a project that was completely free of cost.

5.4.10 FBCTF

Facebook CTF was tested during development of OTnetic, but platform was abandoned in favor of CyTrONE, as the project was no longer maintained and attempted setup resulted in errors due to issues with the virtual machine engine used for deployment, which is not maintained as of 2019.

5.5 Python CLI Application

As mentioned previously, CyTrONE offers access to virtual machines hosted in a sandbox environment. These machines can be accessed using VNC and provides the users with a command line interface. Since most users have little to no experience using a terminal emulator, a text-based CTF-like application was created. This application guided the users through a series of challenges including, but not limited to, different password cracking techniques and bad security practices, such as leaving sensitive information in plain text on the desktop, and using the same password on multiple services.

The reasoning behind using a command line interface was giving the participants an opportunity to feel as if they were actually hacking. Additionally, it does not harm the system if a user manages to break the application or the cyber range itself as everything can re-instantiated by destroying the cyber range, and executing two other scripts. The scripts will instantiate a new cyber range and copy the newest version of the CLI-application to the appropriate virtual machine in the cyber range.

5.5.1 Story-based Training

The users were guided through a story, where the user took the role of an adversary breaking into a misconfigured Raspberry Pi connected to an enterprise network. The application provided new challenges as missions, where each mission focused on a specific aspect of good and bad security practices related to password use.

The user worked with limited set of basic commands to complete each mission. The first few missions provided the user with relevant commands to complete the mission, but as the user progressed, the difficulty increased, which resulted in less assistance for each mission. The intention behind this was to let the users get familiar with the different commands and how they worked before using them independently. CLI can be an intimidating interface for new and inexperienced users, resulting in a need for a beginner-level introduction to using a CLI-based application. However, the focus was not on learning to use the command line, but rather to complete the missions and give the training a unique touch to make it more memorable.

5.5.2 Challenges

The challenges, referred to as missions in the application, have been carefully designed to supplement the quiz. Furthermore, as the application does not communicate directly with CyLMS, using the cyber range is mandatory to answer a few of the questions given in the quiz.

Each challenge, or mission, requested the user to retrieve something of potential value (e.g. passwords, flags, etc.). The first few challenges were considered as entry level exercises, where the application guided the users by displaying what commands are necessary to complete the challenge. As the user progressed through the different challenges, the application provided less guidance and the user had to apply what they learned in the previous challenges.

5.5.3 Code Quality

The code should be of high quality, as the CLI application may be developed further. The different components used for building the application consist classes which do not communicate directly with each other to have a low degree of coupling. This will also allow for bigger changes in the code, as well as replacing a component without breaking the application. The application was built using the PEP8 coding standard for Python to increase the readability for potential future developers of the application.

5.5.4 Target Environment

The participants interacted with one of the virtual machines in the cyber range, called "red". This virtual machine was used to communicate with another virtual machine in the cyber range, presented as the target machine. Furthermore, CyTrONE allows for a variety of operating systems to be installed and hosted on virtual machines instances in the cyber range. Currently however, CentOS 7 is the only image installed in CyTrONE's disc image library. The training environment is almost identical to a typical home-folder in Linux with different folders such as "Desktop", "Downloads", "Pictures" etc. However, as the majority of the participants are from Norway, all of different the folders and files constructing the environment are named in Norwegian.

5.5.5 Creating a New Training Module

The CLI-application takes a single JSON-file as input for managing the training content (exercises/missions), allowed commands, training environment, users and flags. Creating a new training module for the CLI application requires a few hours of time given that the lecturer is familiar with JSON-format and basic IT concepts such as IP addresses, users and file systems.

5.5.6 Attack Simulation

The CLI-application simulates a few commonly known password attacks. These attacks have been simplified to make them more understandable for the end-users. For example, during the process of cracking a password, one would compare hashes, which means each password attempt will be hashed and then compared to the hash of the password being cracked. In the CLI application, this process has been simplified so that the password attempt is being compared to the password in plain text. Two password attacks are visualized in the cyber range. These attacks includes a brute force attack and a dictionary attack. The brute force attack simulation exemplifies how an adversary can crack a relatively short password consisting of up to four letters in a short amount of time. The dictionary attack simulation exemplifies how an adversary can use a word list to crack a password that only consists of a few words.

5.6 Method for Evaluation of the Artifact

The evaluation phase, detailed in chapter 6, was performed after defining the requirements and design of the artifact and completing the implementation of the OTnetic training program. The artifact was evaluated based on predefined evaluation metrics and responses to a questionnaire issued before and after the training. The evaluation metrics reflect the purpose of the OTnetic training program and to what extent it is a superior to alternative training methods.

5.6.1 Lab Experiment

Evaluation of OTnetic was performed based on the results from the lab experiment. Hevner, March, Park, and Ram (2004) describe five primary design evaluation methods. The five methods are (1) observational, (2) analytical, (3) experimental, (4) testing and (5) descriptive. Lab experiments fall under the third category, and is described as a method where the artifact is studied in a controlled environment for qualities like usability. Black box testing, which falls under the fourth category, was employed prior to conducting the lab experiment in order to identify potential bugs that would hinder completion by the lab experiment participants. Lab experiments as an evaluation strategy is also supported by Venable, Pries-Heje, and Baskerville (2016), who separate design evaluation methods into two categories: artificial and naturalistic evaluation. Furthermore, they state that artificial evaluation strategies, such as lab experiments, simulations and theoretical arguments are better suited for evaluating hypotheses and artifacts that are technical in nature. Moreover, artificial evaluation strategies like lab experiments have the benefit of stronger scientific reliability in the form of better repeatability and falsifiability (Venable et al., 2016). Based on these two articles, a lab experiment was found to be the most appropriate method for evaluating the OTnetic training program. The lab experiment featured two groups of nine participants. The OTnetic group is referred as group A, and the lecture group is referred to as group B.

As mentioned previously, the first group (A) used OTnetic as their training program, and the second group (B) were provided with a traditional training method used in the Norwegian energy sector. This training was issued in the form of lecture with one-way communication, which is a common method for training employees. Due to the COVID-19 pandemic, it was not be possible to hold a physical lecture. Moreover, in order to allow participants complete training at their convenience, and to keep the lectures consistent, a pre-recorded video lecture was produced in addition to the artifact, which was sent to the lecture group. The video was uploaded to YouTube as a private video so it could be viewed by participants without requiring them to download any files or video playback software. In order to fairly evaluate the two training methods, the video lecture focused on the same topic, and provided the same information as the sample training module for the cyber range training program.

The lab experiment provided insight into whether the artifact is more effective than traditional training methods for OT personnel or not. In order to evaluate the learning output of each training method, participants were issued a questionnaire before and after participation in their respective group's training program. The questions in the questionnaires were identical, with the exception of additional questions in the post-participation questionnaire pertaining to the participant's experience with using the training program. By comparing each participant's post-participation questionnaire results with their respective pre-participation results, it was possible to ascertain whether or not the program increased the participant's knowledge of the chosen training topic. To assign a score to each participant, every question in the questionnaire was assigned a point score. Questions with multiple correct answers had one point per correct answer to the question. This means that a participant could gain one or more points per question, depending on the questions. Questions that were qualitative in nature, such as ones pertaining to the participant's subjective experiences of the training, were not assigned a point score.

Participant Selection for the Lab Experiment

During the interviews performed in study, it was found that there is a general lack of cyber security knowledge among OT-personnel, and that they do not receive cybersecurity training more regularly than once a year at most. Based on these findings, there is little reason to believe that a person who does not work with OT, is better or worse suited to complete the training program than an OT-employee, as long as the participant does not work in IT. Furthermore, the selected participants expressed that they are generally not interested in cyber security, which aligns with the interview findings. Therefore, as they fit the profile of the target group, people who do not work in IT or have a degree in IT, were considered eligible to participate in the lab experiment.

The lab experiment was performed with a total of 18 participants, 9 in group A, and 9 in group B. Table 5.1 illustrates the demographics of participants in the lab experiment. Furthermore, there was a somewhat even gender distribution, with 11 male participants, and 7 female participants. Each participant was also asked to provide a subjective rating of their own IT competence level on a 5-point Likert scale. As table 5.1 shows, the lab experiment participants were on lower end of the spectrum. However, it was found that the participant's own assessment did not necessarily correlate with their performance during training.

	Age				Gender		IT Competence				
	19-24	25-35	36-50	50+	Male	Female	1	2	3	4	5
OTnetic	2	4	1	2	7	2	3	2	3	0	1
Lecture	3	2	1	3	4	5	2	1	5	1	0

Table 5.1: Lab Experiment Participant Demographics

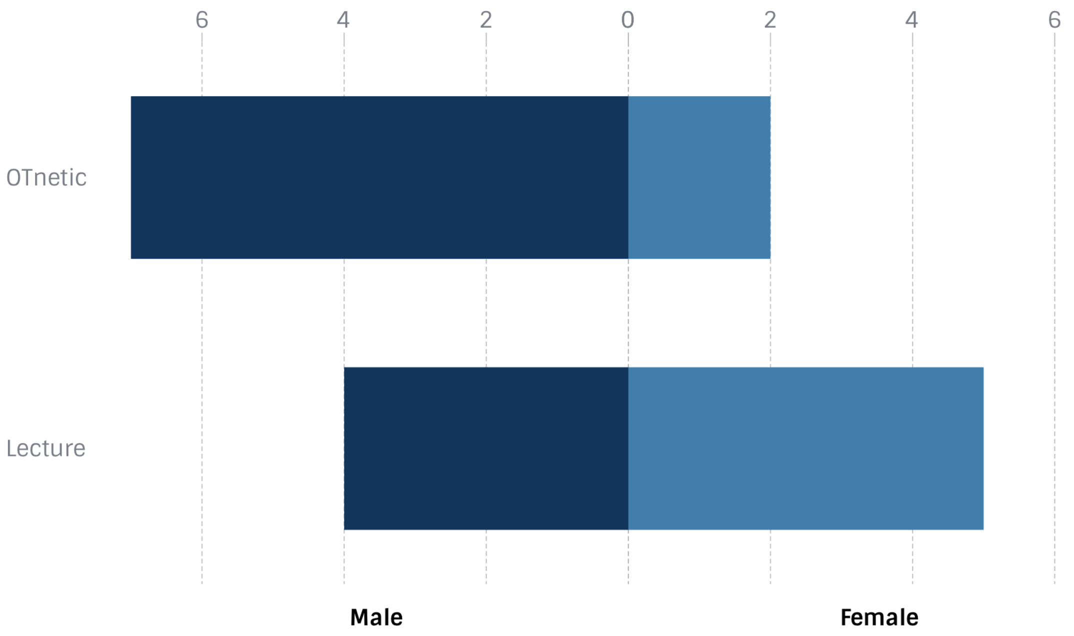


Figure 5.8: Gender Distribution Per Group

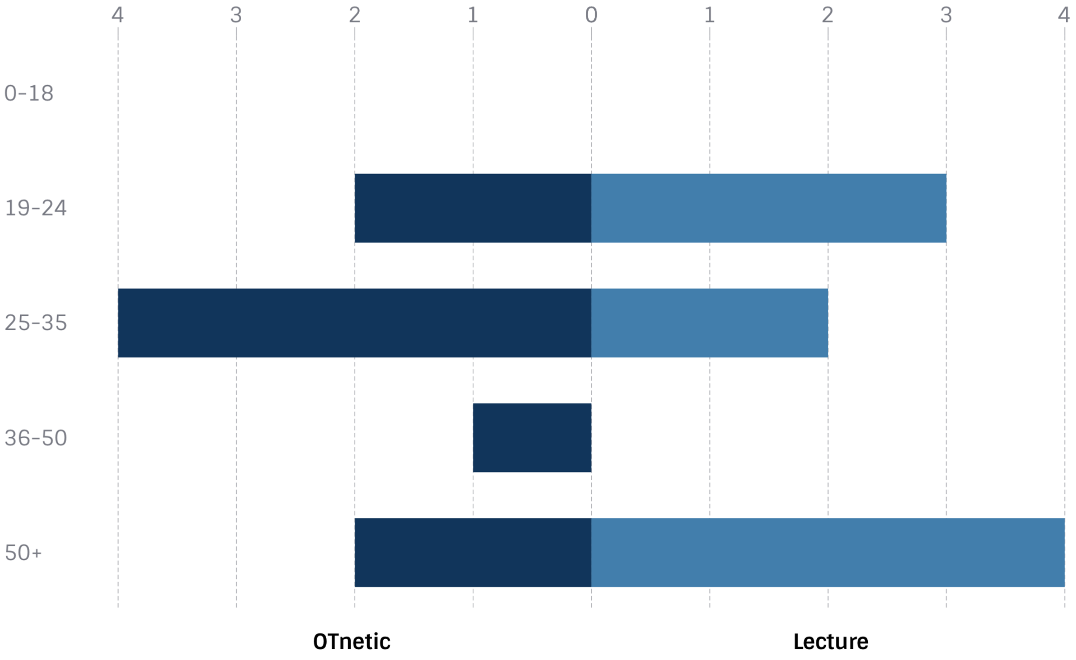


Figure 5.9: Age Group Distribution Per Group

Pilot Test

Before the lab experiment could be completed, a pilot test was performed in a controlled environment, using students as test subjects. The primary objective of the pilot test was to establish a standard procedure for performing the lab experiment. Furthermore, the pilot test uncovered bugs and misspellings in the OTnetic cyber training framework that were addressed before the final lab experiment. Moreover, the pilot test was done to ensure that the OTnetic training program would work well when used by a participant without an IT background. Participants were considered to not have an IT background if they do not have an IT-oriented education or technical IT-related tasks as part of their work. In other words, people who do not work in IT or have a degree in IT, were considered eligible to participate. Another goal was to be able to gauge the difficulty level of the program, and identify how long it would take to complete the entire program, which is why participants with little prior knowledge was preferred.

During the pilot test, it was found that the average target participant, with no IT education or IT related work tasks, used between one and two hours to complete the entire training program. The long completion time was due, in part, to the pilot test participants struggling with some of the more difficult tasks. However, they did not report that the training program was too difficult, or too easy. The two pilot test participants reported that the difficulty level was at 3 and 2 respectively, on a 5-point Likert scale.

The pilot test yielded encouraging results, and feedback was given by each participant. Users were positive to the program, and described it as interesting and more fun alternative to lectures. The program's practical tasks and objectives required the user to actively participate, and it was clear through observation that the pilot test participants were actively engaged while using the training program. During the pilot test, some bugs were discovered. These were fixed immediately, so the next pilot test participant would not encounter the same bugs. Therefore, the first test user experienced more bugs than the last. However, time spent fixing bugs was deducted from the participant's over time usage.

Lecture Based Training in the Energy Sector

The authors of this thesis attended a cyber security preparedness exercise organized by a cyber security consulting company. This exercise consisted of a lecture part, and a discussion part where participants were able to contribute by sharing their own experiences and challenges related to cybersecurity issues and incidents. There were about ten participants in addition to the organizers. The participants consisted of IT professionals and managers from different energy production companies.

As this training was directed towards IT personnel and managers dealing with security incidents, the training content was considered too advanced for OT personnel. However, as this project focuses on the training delivery method, the same training model that was used in the exercise will be applied, with more basic training content and by delivering one-way communication exclusively.

Hypothesis

For the lab experiment, two hypotheses were defined:
Hypothesis 1 (H_1): using cyber ranges as a training method is more effective and motivating than traditional training delivery methods including lectures.
Null hypothesis (H_0): there is no difference in effectiveness and motivation between the different training delivery methods.

Furthermore, the following null hypotheses, indicated by figure 5.10, were formulated in order to assess whether a change of cybersecurity awareness and knowledge had occurred or not:

1. There is no improvement of cybersecurity awareness and knowledge at T-1 compared to T-0 among members of the intervention group
2. There is no change in cybersecurity awareness and knowledge at T-1 compared to T-0 among members of the control group

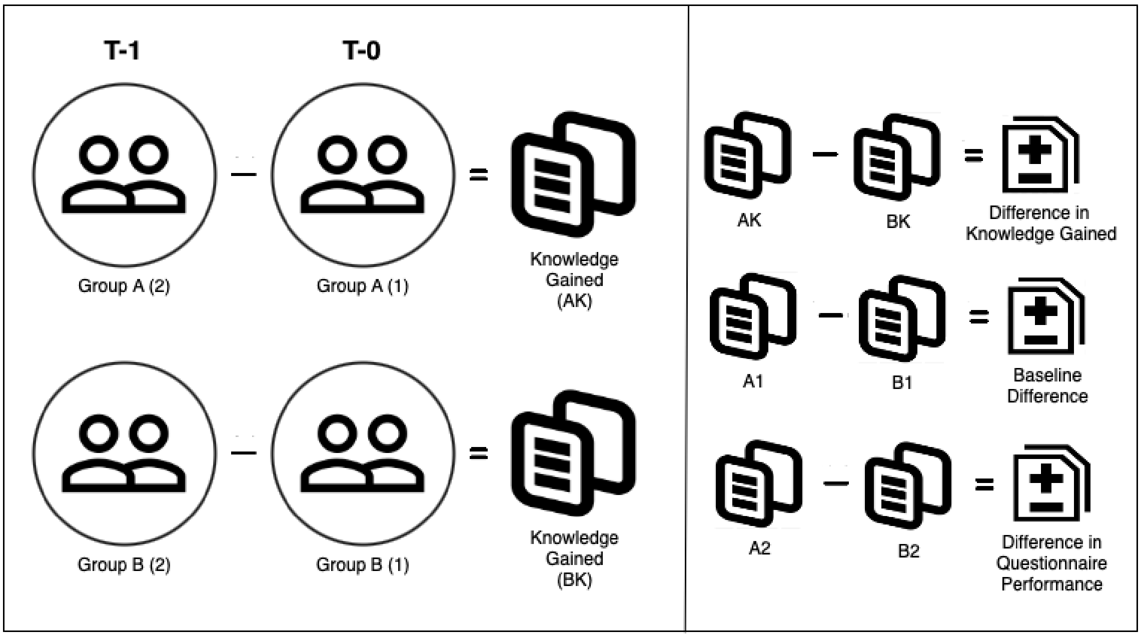


Figure 5.10: Lab Experiment T-test
Group A: OTnetic trainees
Group B: Lecture trainees
T-1: After treatment
T-0: Before treatment

5.6.2 Questionnaire

Prior to, and following the lab experiment, a questionnaire was issued to participants based on the evaluation metrics defined in subsection 5.6.3. The evaluation metrics were derived from the literature review and interviews performed as part of this thesis. The primary purpose of the questionnaire was to evaluate the user's overall experience with the training program, the quality of the training content, changes in the participants attitudes towards the importance of cyber security, and the knowledge they gained. The participants' qualitative evaluation of the training program, in addition to the quantitative results of their performance improvement on the questionnaire, formed the basis for the artifact evaluation.

5.6.3 Evaluation Metrics

The evaluation metrics for the training program reflect upon how well the artifact serves its intended purpose, and how the participants perceived the training experience. For the purposes of evaluating the training program, two main categories have been defined; software metrics and training content metrics. The two categories have their own evaluation metrics, some unique and some common, that together form the evaluation basis for the training program. By diving the evaluation metrics into two categories, it is possible to identify the efficiency of the artifact as a whole, in addition to evaluating the training content and cyber range software separately. This ensures the possibility to identify whether a positive or negative evaluation stems from issues with the practical use and quality of the cyber range software, or from the training content that was created. As mentioned previously, participants were asked to fill out a questionnaire before and after participation in the training program. The pre-participation questionnaire only included questions designed to identify the participants' attitudes towards cybersecurity issues, motivation to comply with security policies, and their current knowledge level of the security concepts in the training content. The post-participation questionnaire contained both knowledge, motivation and security attitude questions, in addition to questions regarding usability of the training delivery method and relevance of the training content they were given.

According to Albrechtsen and Hovden (2010), the quantitative analysis of an intervention should be supported by qualitative evaluation techniques, as qualitative approaches provide a depth to the evaluation that cannot be achieved by using quantitative methods exclusively. Free-text data from the second questionnaire was used for this purpose, with the aim of receiving information regarding why the training program influenced security knowledge and attitudes, and if the program itself was motivating, engaging, and easy to use. Furthermore, the qualitative questions on the questionnaire allow for comparison between the training program and alternative training approaches as delivery methods for the training content. Thus, it is possible to discern if motivation to change security related behavior is connected to the delivery method of the training content. Moreover, the participants' experience with the training program could negatively affect their motivation and knowledge acquisition.

This could be caused by usability issues with the training program, which is caused by the program itself, instead of the training approach.

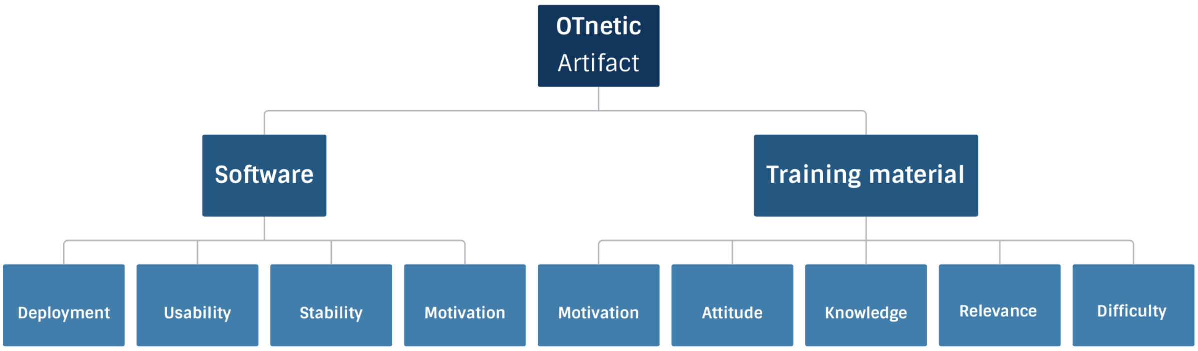


Figure 5.11: Evaluation Metrics for OTnetic

Figure 5.11 illustrates the metrics which have been chosen for evaluating the quality of the software and the training content respectively. These metrics are described further in appendix G.

5.6.4 Evaluation of Data Quality

In order to ensure a certain quality related to the data collected from the lab experiment and the interviews, a set of requirements were created. These requirements ensure that data collected from the lab experiment is suitable for use in future analysis. The requirements were selected based on Pipino, Lee, and Wang's (2002) suggestions for data quality dimensions, where the metrics relevant for this project were selected. The following requirements were established to ensure high quality regarding data collected during this project.

1. Accuracy: The collected data must be accurate.
2. Relevancy: The collected data must meet the requirements for the intended use.
3. Completeness: The data should not have missing values or miss data records.
4. Timeliness: The collected data should be up to date.
5. Consistency: The collected data should have the data format as expected and can be cross-referenceable with the same results.

Chapter 6

Artifact Evaluation

This chapter presents the results gathered from the lab experiment described in section 5.6.1. The results were gathered from the questionnaire that was issued to each participant before and after completing their training sessions. The results consist of a quantitative part, and a qualitative part. As mentioned in chapter 3, the questionnaire questions were assigned a point score in order to evaluate the increase in knowledge per group. The two groups are referred to as group A and group B. Group A received the training program developed during this project, called OTnetic. Group B received the pre-recorded video lecture, also produced as part of this project. Both groups received the same information, and the same questions in the lab experiment questionnaires.

6.1 Quantitative Evaluation

This section presents the quantitative results from the lab experiment. This includes the results from questions that were given a point score. Section 6.2 presents the qualitative results, which includes the participants' subjective evaluation of the training program.

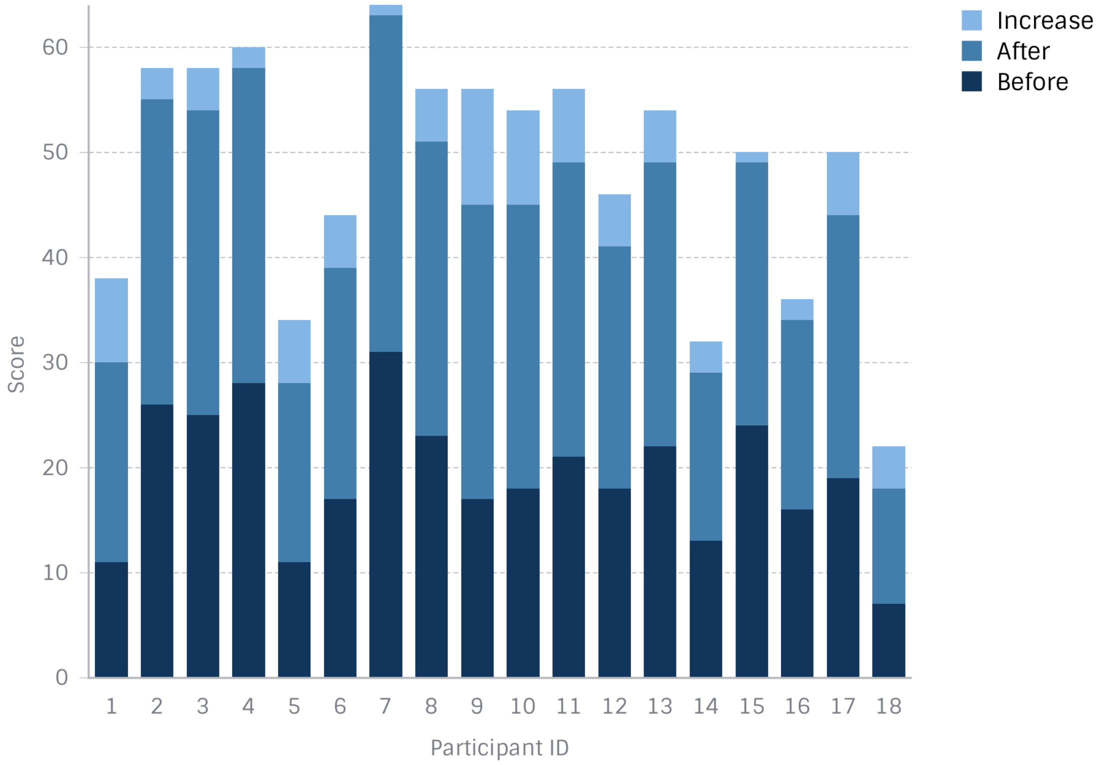


Figure 6.1: Knowledge Improvement Per Participant

Figure 6.1 illustrates the score achieved by each participant before and after training, as well as their improvement. The IDs ranging from one to nine belong to group A (OTnetic), while IDs ranging from 11 to 18 belong to group B (lecture).

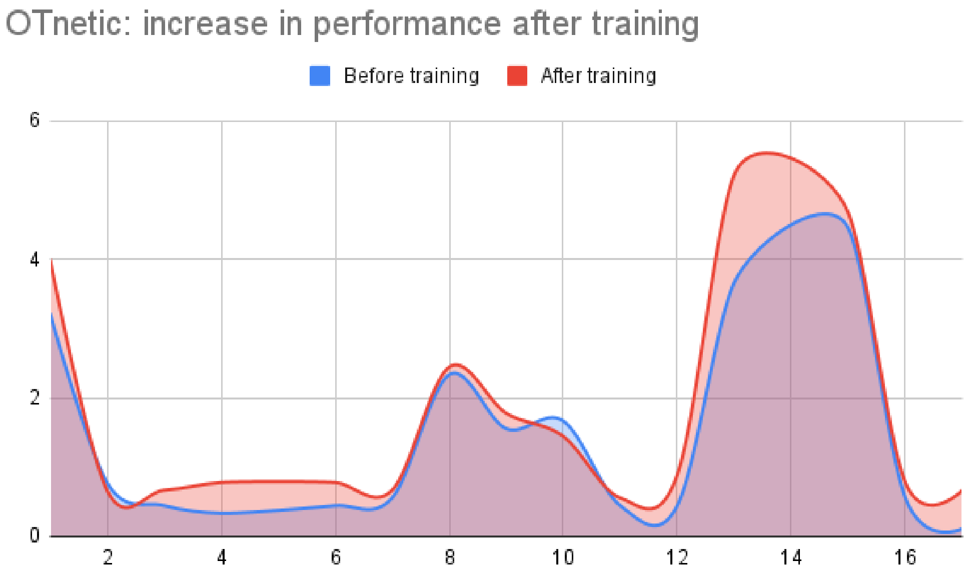


Figure 6.2: Performance Comparison Before and After Training for Group A

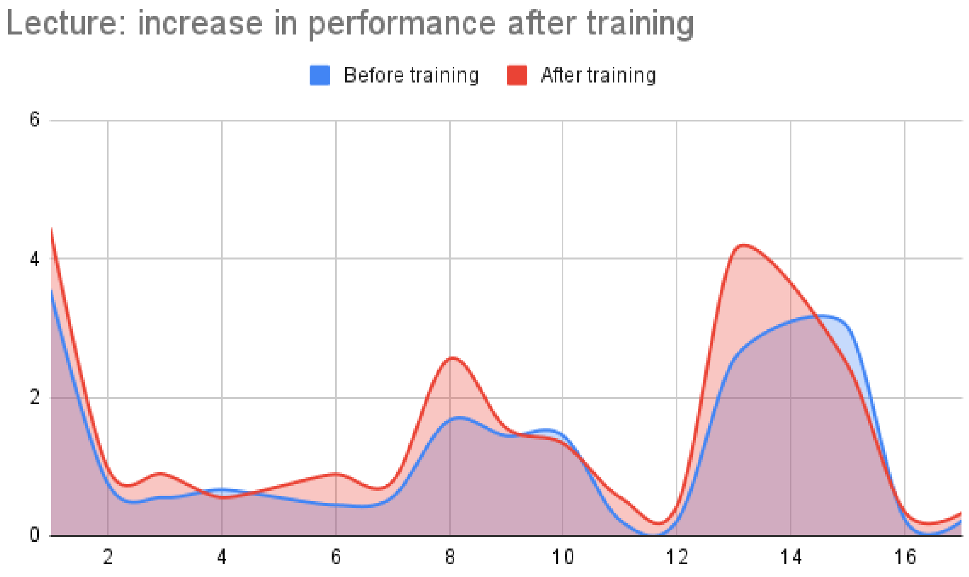


Figure 6.3: Performance Comparison Before and After Training for Group B

Figure 6.2 and 6.3 illustrate the mean score per question answered by each group before and after training was provided. The blue marks the performance before the training, while the red marks the performance after the training. As the figures illustrates, both of the training approaches led to a higher mean score for some of the questions.

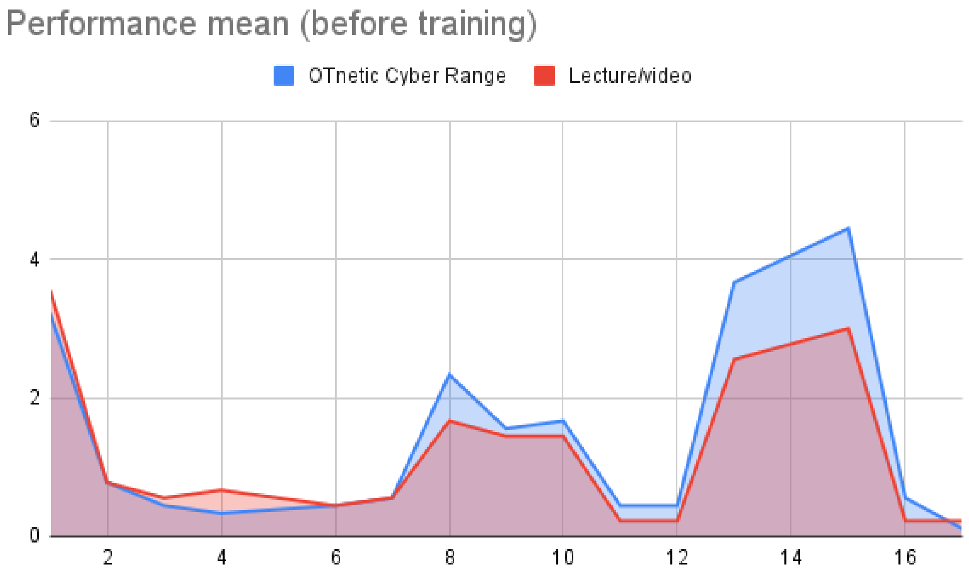


Figure 6.4: Comparing Mean Performance of Each Group Before Training

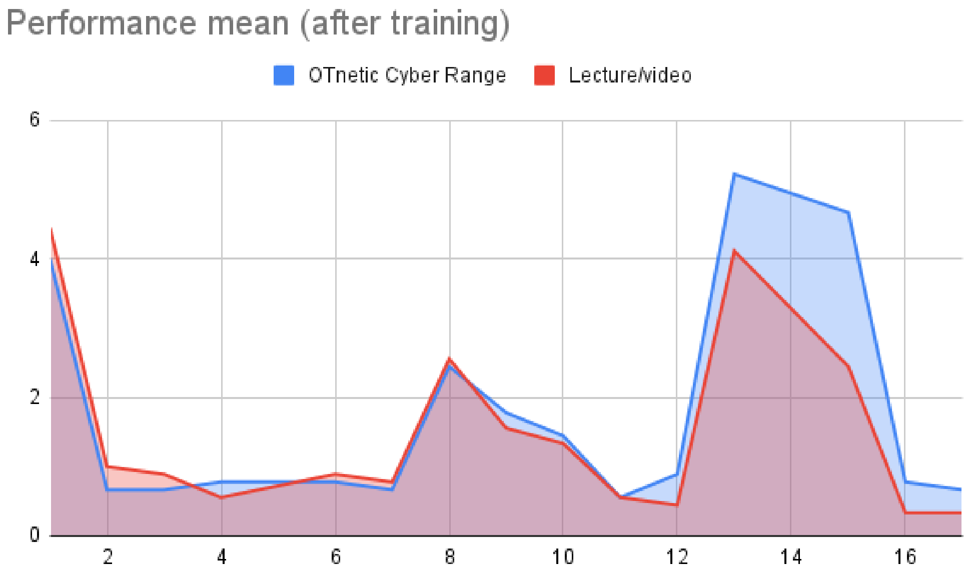


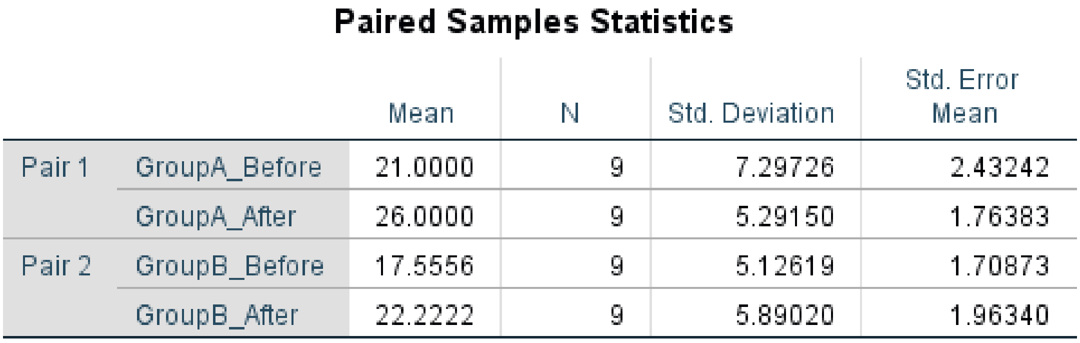
Figure 6.5: Comparing Mean Performance of Each Group After Training

Figure 6.4 and 6.5 compare the mean score for each group before and after the performing the training. These figures are quite similar to figure 6.2 and 6.3, but instead of showing performance increase before and after training they are directly comparing the performance between the two groups. As figure 6.4 shows, group A had more correct answers than group B in the questionnaire for establishing baseline knowledge. Furthermore, we can see that there was a small improvement for both groups after the training.

6.1.1 Paired Sample T-Test

A paired t-test was employed in order to compare mean performance between group A and B. This form of test was performed to measure the effectiveness of the OTnetic training program and compare it with lecture-based training. As mentioned in section 5.6.2, a pre-test was conducted in order to establish a baseline of the participants' cybersecurity knowledge. After completing the training, the participants took a post-test questionnaire in order to provide a point of comparison that could be used to establish the participants' knowledge increase. The knowledge increase was determined by calculating the difference of the post-test score from the pre-test score of each participant. Statistical Package for the Social Sciences (SPSS) was one of the tools used to analyse the results from the t-test. The results from the t-test were included in the thesis as they supported the findings from the non-parametric test. However, a t-test should be conducted with a larger sample size as this is a pre-requisite for this type of statistical test. Additionally, the data used for the test should be normally distributed. This test is included, despite the low sample size, as it provided results that supported the results from the Mann Whitney U test.

The Paired Samples t-test compares the means of two measurements taken from the same individual, object, or related units (Kent State University, 2021). These "paired" measurements can represent things like: A measurement taken at two different times (e.g., pre-test and post-test score with an intervention administered between the two time points). A paired samples t-test should be conducted using data that is normally distributed. For this thesis however, it was unknown if the data was normally distributed due to the sample size. Regardless, it was decided to include this test as this thesis is exploratory, and the test could reveal if the training had an effect if combined with other tests that are able to account for the potential lack of normal distribution. A non-parametric test has been conducted as well, as this will account for the limitations of the paired sample t-test. The non-parametric test, called a Mann Whitney U test, is described in section 6.1.2.



Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	GroupA_Before	21.0000	9	7.29726	2.43242
	GroupA_After	26.0000	9	5.29150	1.76383
Pair 2	GroupB_Before	17.5556	9	5.12619	1.70873
	GroupB_After	22.2222	9	5.89020	1.96340

Figure 6.6: Results from T-Test Analysis with Both Groups

Figure 6.6 describes the mean performance for both groups before and after training, in addition to the standard deviation. Furthermore, a difference in mean performance between the pre-test and the post-test may indicates that the training had an effect on the performance. The standard deviation reveals how close the participants were to the mean score of its own group, indicating how consistent the increase or decrease in performance was across the entire group.

6.1.2 Mann Whitney U Test

In addition to the T-test, a non-parametric test called the Mann Whitney U test was performed. A non-parametric test was performed due to the small sample size and data set used does not assume normal distribution. The test calculation used a two-tailed test with a significance level of α 0.1. The test calculated a P-value of 0.07632 for the results after training. Since the P-value is greater than α, H_0 is rejected. To summarize, the test shows that hypothesis 1, which states that using cyber ranges as a training delivery method is more effective and motivating than traditional training methods, is supported. The three figures below present the results from running the three different tests in figure 5.6.1. Figure 6.8 shows the median test scores of group A and B after training. Figure 6.7 shows the median test scores of group A and B before training.

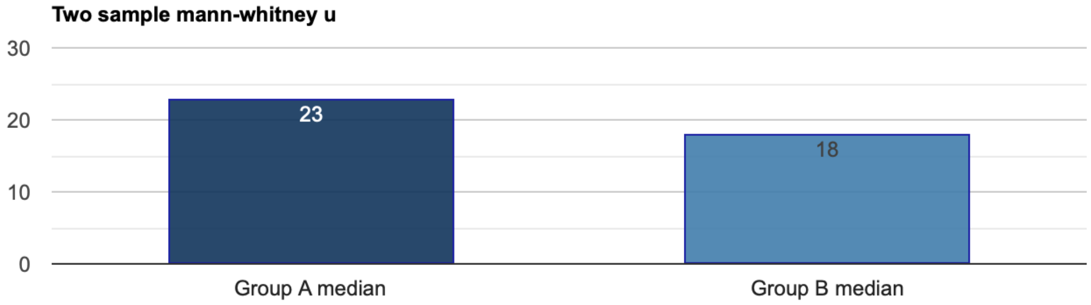


Figure 6.7: Two Sample Mann Whitney U Test for Group A and B Before Training

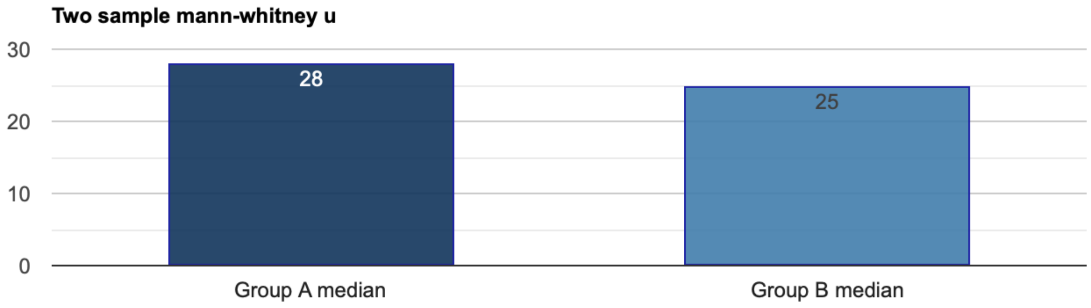


Figure 6.8: Two Sample Mann Whitney U Test for Group A and B After Training

6.2 Qualitative Evaluation

As mentioned previously, each participant was asked to evaluate the training they received in terms of relevance, difficulty, motivation, and how efficient the program was at teaching cyber security. Moreover, every participant was asked to provide some feedback regarding what the participant liked about the training they received.

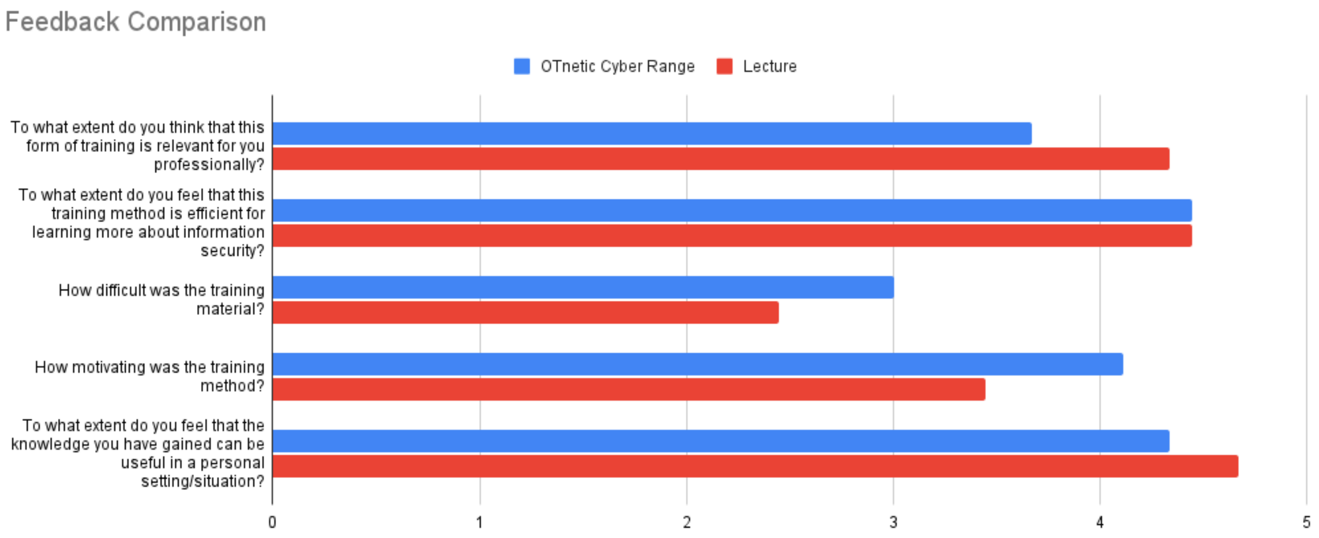


Figure 6.9: Comparing Feedback from Groups A and B

Figure 6.9 describes the feedback provided by both groups. A potential limitation with this feedback is that it is based on the participants' subjective opinion. However, the participants' personal experiences are important to consider as they may reveal deficits in the training delivery method or the training content itself.

Chapter 7

Discussion

This chapter provides discussions and reflections regarding the results presented in the previous chapter. Furthermore, the thesis' contribution to research and practice is illustrated, and limitations of the study are presented.

This thesis has examined various training methods and open source programs that can be used create a cyber range platform. As mentioned in section 3.1, the activities formulated by Peffers et al. (2007) were used during the design and development of the artifact. OTnetic was developed and evaluated based on the needs and requirements of organizations in energy sector, and is well suited for training in such organizations. The need for additional cyber security training was identified in the interviews performed in the thesis, as well as Giuliano and Formicola's (2019) findings presented in the literature review. Based on the results of this study, it is worth exploring cyber range based training further. As both training methods resulted in better scores for all of the participants in the lab experiment, there is reason to believe that a combination of the methods may be ideal. Therefore, further development of OTnetic will likely include short videos introducing the training content as part of the training program. This solution would reduce the need for text-based explanations of the training topics.

7.1 Limitations

As mentioned previously, in this project, only one round of the DSR cycle was performed due to time constraints. Ideally, several more iterations of the cycle would be completed in order to continuously improve the artifact with feedback from the users after each completed cycle. However, further research and development is expected. Plans and ideas for further development are outlined and described in section 7.4.

Additionally, limitations related to the COVID-19 pandemic need to be considered. Due to the current pandemic, it was not possible to perform in-person interviews. Moreover, it was not possible to perform the lab experiment in person, without taking the necessary precautions needed to ensure the safety of the participants and the lab experiment instructors. The solution to this issue was to perform the interviews online, and to allow lab experiment participants to perform the training program online, from their homes. Furthermore, the control group received a pre-recorded video lecture, instead of a classroom lecture, which may be beneficial. As mentioned in the literature review, cues such as reactions of others, speaker credibility and the attractiveness of the speaker can affect the trainee's perception of the lecture (Puhakainen & Siponen, 2010). These factors should be alleviated by the use of a video lecture where the speaker is unknown and the trainee is watching the lecture alone. Despite being a limitation, the video lecture and online lab experiment offers increased flexibility to participants, and is more consistent in cases where participants may need to complete the lecture on different days. Moreover, this type of training is likely to become increasingly popular, as an increase in working from home is likely to persist as a result of a shift in work culture caused by the COVID-19 pandemic.

Another potential limitation is that it may be difficult to get accurate and elaborate answers to interview questions, due the sensitive nature of the intended questions. Organizations may be sceptical when it comes to providing students with information, especially as it relates to their internal security. However, this issue was mitigated by signing a non disclosure agreement with the client organization stating that power sensitive information would not be included in the thesis, as well as providing an assurance of anonymity to interview subjects and their respective organizations.

As the study was conducted using a small sample size, the results may be caused by other factors. Since a single participant's score accounts for a ninth of the calculated mean, one participant can potentially have a drastic impact on the mean performance of the entire group. Both the paired samples T-Test and the Mann Whitney U test have a statistical significance. There is reason to believe that the differences in increased knowledge in the two the groups are caused by the treatment they received.

Another potential limitation regarding the lab experiment is the difference in time duration related to the two training methods. The participants using the OTnetic training framework trained for about an hour or longer, while the video only lasted about twenty minutes. Despite the fact that this makes for a difficult comparison, research suggests that the process of active learning is in itself more time-consuming than participating in a meeting or a lecture. However, if the objective is to give the participant an opportunity to understand and master the information, active learning is more effective than lectures and classroom-exercises such as tabletop discussions (Hackathorn, Solomon, Blankmeyer, Tennial, & Garczynski, 2011).

Lastly, as this project only includes six interviews, which is a small sample size, there is a limitation of whether or not the viewpoints and information gathered from interviews provided a comprehensive understanding of the security situation for the entire energy sector.

7.2 Analysis of the Results

The hypothesis for this thesis states that using cyber ranges as a training delivery method is more effective and motivating than traditional training delivery methods, such as lectures. This hypothesis is supported by the results presented in the previous chapter. However, the differences in learning output were smaller than expected. This could be explained, in part, by the small sample size of the lab experiment. Moreover, the fact that group B (lecture) had lower pre-training test scores, means that they had more room for improvement than group A (OTnetic). However, a better score on the pre-test may suggest that participants in this group are better equipped to learn new information security concepts. As group B had a lower initial score than group A, they had more potential points to gain in the post-training scores. Furthermore, the standard deviation from the T-test presented in figure 6.6 suggests that group A had a more consistent performance increase as the mean score increased and the standard deviation decreased after the training. However, we are unable to determine if this decrease in the standard deviation for group A is coincidental or caused by the treatment. These two parameters suggests that all the participants in group A had a score closer to the mean score of the group after the training. For group B however, the standard deviation increased after the training suggesting that the increase in performance may not be as consistent for the entire group.

The lab experiment conducted in this thesis was formed in accordance with the UCIT model presented by Puhakainen and Siponen (2010), which was described in the literature review. The process starts with determination of the instructional task, which was created in OTnetic prior to the lab experiment. Then, the trainee's current state was diagnosed with the questionnaire. After delivering the training, the trainee was reassessed with the second questionnaire, and the success of the artifact was diagnosed. Furthermore, Puhakainen and Siponen (2010) also mentioned that the training content should be personally relevant for the learner, as motivation is a prerequisite for cognitive processing. This was taken into account when developing the training content, as it was also mentioned in one of the interviews. Additionally, it was identified in the literature review that employees often struggle to understand the consequences of bad security (Karjalainen & Siponen, 2011). OTnetic attempts to demonstrate the consequences of poor password habits by allowing trainees to perform attacks that show how easily a hacker can crack weak passwords. This knowledge is applicable in the trainee's personal and work life.

The results show that all lab experiment participants learned something new, as all of them performed better on the post-training test. This reveals that both training methods will provide untrained employees with new knowledge, unless the participants dedicated their own spare time learning more about password security, which is unlikely considering that the post-test was provided the next day. However, OTnetic allows trainees to perform practical tasks and active learning, which can be more effective at creating long-term knowledge. Moreover, OTnetic may be suited for more difficult training content or specific topics. As discussed previously, active learning is better for learning specific topics with a limited scope. Furthermore, more advanced topics than the one presented in this thesis may be present itself as better use case for OTnetic, as difficult topics would benefit more from active training and practical tasks.

As mentioned in section 2.2.2, Beuran et al. (2017) have established a set of five requirements that make an effective cyber security training program. The first three requirements are fulfilled by the OTnetic training program. Firstly, OTnetic contains appropriate training content for the target audience in terms of knowledge and ability levels. Secondly, the training program contains training content corresponding with the skills the program aims to develop. Lastly, it uses hands-on activities and exercises to make the training more memorable and realistic. The final two requirements of reaching a large audience to generalize the training and have sufficient cost contra performance characteristics to make the program sustainable in the long term, where not fulfilled as the cost-efficiency has not been tested and the training content is tailored for a specific target audience.

The cyber range is currently accessible through a command line interface. Utilizing this interface requires an introduction, as some participants found it to be hard to use and understand. This is because many users have never been required to interact with a terminal emulator before. However, many of the participants reported that using this type of interface was an overall positive experience, and that they learned a great deal from using it. Moreover, the use of a terminal made the training feel like a game according to some participants. Additionally, most of the participants who used OTnetic reported that the program was motivating, as opposed to the lecture group, which reported less interest in the training. The results from the lab experiment indicate that a short video about the topic can be beneficial in combination with the OTnetic training program. OTnetic could be modified to include short video introductions explaining topics before the practical session in the range, which would require less text to be presented to the trainee. A video on the use and benefits of the terminal may also presented to trainees in future, in order to make the program more approachable. Additionally, training with OTnetic may be better suited for learning more difficult material that is hard to teach in a lecture, or requires the trainee to learn a concept that is practical in nature. As table 5.1 illustrates, all the participants in the lab experiment were asked to evaluate their own IT competence. However, it was found that the participants' own assessment of their IT knowledge did not correlate with their test scores. The users that claimed higher competence did not score any better than the users that claimed to be on the lower end of the spectrum.

Overall, the group that performed the OTnetic training program provided much more positive feedback when asked what they thought was positive and negative about the training they received. Participants from group A reported that they have become more aware of cyber security issues and the importance of secure password habits, how to create strong passwords that easy to remember, the importance of multi-factor authentication, and how to identify phishing attempts. Moreover, these participants felt that the training was clear and logical. Unlike the lecture group participants, OTnetic's users reported that the training was fun, engaging and motivating. The combination of quiz questions and practical tasks with a flag based scoring system was very motivating, according to the participants. They also liked being able to execute commands in a Linux system, and the ability to see examples of how hackers are able to crack passwords. Furthermore, one participant stated that the training program was challenging enough that it was not boring to perform, and that it reminded them of a text-based adventure game. These results align well with the findings from the literature review (2.2.2), as elements from gamification have proven to increase motivation if implemented properly according to Paton and Jackson (2002). The utility of gamification is further supported by Adams and Makramalla's (2015) research which is presented in the literature review. Furthermore, the feedback from group A aligns well with the evaluation metrics proposed for the artifact in figure 5.11.

Despite the participants in the lecture group also improving their knowledge of password security from training, they reported that the passive learning style provided by the lecture made it difficult to remember the training content. Furthermore, some participants mentioned that the video was too long, which made them lose focus and motivation to complete the training. Despite participants in Group A spending one to two hours on their training, none of them reported that the training session was too long. In comparison, the video lecture presented to group B was about twenty minutes long in total. As figure 6.9 illustrates, when asked how motivating the training method was, group B rated their training at an average of 3,4 on a scale from one to five. Group A rated their motivation at an average of 4,1. The difference in motivation between the two groups may be explained by the presence of gamification elements in the OTnetic training framework, which is supported by the literature described in section 2.2.2. Furthermore, regarding the difficulty of the received training method, group A had a mean score of 3, while group B had a mean score of 2,4, suggesting that the OTnetic training framework was a bit more difficult, while still being more motivating. This may suggest that using the cyber range and quiz is more fun than watching a video lecture. One possible explanation for this is the use of gamification in the OTnetic training program. As found in the literature review, gamification makes the learning experience more fun for participants, increases motivation, and produces a greater learning outcome (Adams & Makramalla, 2015). This is further supported by the literature review finding that applying game-design elements and game principles to the training process will enrich the learning experience and motivate trainees. However, these results are based on the participants subjective opinion. In summary, although both groups did show improved knowledge after completing their training, group A showed much higher interest and engagement in their training, and found their training program to be more motivating overall, which according to Puhakainen and Siponen (2010) is a prerequisite for cognitive processing.

7.3 Implications for Research

This research has focused on OT-personnel in the Norwegian sector, as the client organization identified a need for new methods to provide additional cyber security training for this group. OT-personnel work with critical technology, and they have a great responsibility to aid in the organizations ability to maintain a strong cyber security posture. However, by conducting interviews with energy companies, it was found that there is a lack of general IT and basic security knowledge among these employees. Solid password security and habits are essential to protect systems and networks. Therefore, OTnetic was developed with module focusing on password security initially. A lab experiment was conducted to test the efficacy of OTnetic. In order to accurately evaluate the training program developed during this thesis. Two hypotheses were formulated. Hypothesis 1 states that using cyber ranges as a training delivery method is more effective and motivating than traditional training delivery methods including lectures. A null hypothesis was also formulated, which states that there is no difference in effectiveness and motivation between the different training methods. Further research should be done in order to identify the benefit of cyber range training for other roles and domains. Additionally, further research could be done to examine whether or not this type of training is effective at creating long-lasting or tacit knowledge. Furthermore, it would be beneficial to conduct a large-scale lab experiment with a greater number of participants in order to solidify the validity of results, and explore whether or not the difference in knowledge increase is greater between the two groups when a larger sample size is used. Additional groups could also be used to ascertain the effectiveness of a wider variety of training methods compared to OTnetic.

The research presented in this thesis can be of great value to companies in the Norwegian energy sector. The results from the lab experiment indicate that a gamified approach could be an effective alternative to current training methods to increase knowledge retention. Furthermore, the feedback suggests that some of the participants had a more positive attitude towards information security after the training. Moreover, the thesis has contributed to the academic literature landscape by presenting a viable alternative to traditional training methods in the form of cyber range training, which can be used to present new information and allow the trainees to develop practical skills. These skills are valuable assets an employee can use to contribute their organizations cybersecurity posture. Furthermore, the research has identified that cyber range training may be a more motivating training method than lectures. Additionally, this thesis has revealed the issue of lacking cyber security knowledge and skills among OT-personnel in the Norwegian energy sector, and shown that it is possible to create training that elicits internal motivation in trainees that are not necessarily interested in information technology.

Further research on the efficacy of cyber ranges should be conducted in order to better establish the learning benefits of this training method. It would also be beneficial to conduct a lab experiment in greater scale, with more participants and additional training modules. The research presented in this thesis suggests that cyber range training can be a useful tool to teach cyber security to OT-personnel in the Norwegian energy sector. However, it would be interesting to conduct further research that investigates the applicability of cyber range training in other sectors and roles. Moreover, a graphical interface could be more suitable to training employees who do not have a background in IT, as the CLI interface was unfamiliar to some of the lab experiment participants.

As stated in the introduction in chapter 3 the design science research approach has gained popularity over the last years. Furthermore, this approach was well suited for answering the thesis' research questions, and developing and evaluating an artifact with a focus on increasing motivation and developing practical skills. We suggest that DSR could be an effective approach for software development where research is in focus, given that the artifact requirements are dependant on the target audience. Firstly, the DSRM employs a similar incremental model as current software development methods. Secondly, the artifact produced as result of the project would be grounded in previous research given that a literature review has been conducted. Lastly, the results from the project may contribute to other organizations operating in the same domain, as well as different research communities. We believe the thesis has contributed in closing the research gap identified earlier.

7.4 Implications for Practice

Further development of the training content provided by the OTnetic training platform will include adding more graphical content such as videos and images, more CPS-related content to increase the relevance for OT-personnel, and allowing participants to attack each other in real-time. As the latter can be challenging to implement, an alternative can be a virtual machine instance acting as the defending side, as this will illustrate how one can halt or thwart an ongoing attack.

Furthermore, additional elements related to gamification can be implemented. OTnetic's learning management system, Moodle, allows instructors to create badges. These badges can be used as a certificate of completion, as they can be earned by completing a single activity, an entire course including multiple activities. Badges will give the participants a feeling of mastery, as they will earn more badges when progressing and completing additional courses. Other ways to further gamify the training can be to make the program more visual by introducing a graphical interface, a leaderboard where users can compete for the best score, and activating chat functionality within Moodle that facilitates better communication among users.

Software-wise, further development will include improvements and automation related to cyber range instantiation and more simulated attacks illustrating the mechanisms in the attack and how it may impact an organization. Additionally, the possibility to work on other operating systems than Linux CentOS 7 can be implemented, as a terminal emulator can be intimidating to users without a background in IT. It is possible to add other operating systems in the form of disc images to CyTrONE's disc image library, such as Windows. Lastly, more training modules should be developed in order to provide trainees with a greater amount of cyber security training content. As password security was the main focus during this development cycle, only one training activity was created in Moodle. In future iterations, it would be beneficial to create courses containing several smaller training activities that could performed in sequence with increasingly difficult activities.

Cyber ranges are predominantly used to teach cyber security concepts to people who work with or study cyber security. However, this thesis suggests that cyber ranges may be suitable as a general teaching tool for people without an interest in cyber security. Moreover, OTnetic's focus on active learning has been shown to be effective, and may be beneficial for organizations to explore alternative training methods that incorporate active learning to increase cyber security awareness in their employees.

Chapter 8

Conclusion

This chapter presents conclusions based on the results presented and discussed in the previous two chapters. The goal of this thesis was to answer the following two research questions:

- How can cyber ranges be utilized as a cyber security training tool for OT-employees in the energy sector?
- What limitations exist in current practical training exercises and programs related to cybersecurity preparedness in enterprises in the Norwegian energy sector?

In order to answer these questions, a training program for improving cyber security preparedness in the Norwegian energy sector called OTnetic was developed. The program was tested against a pre-recorded video lecture in order to evaluate its efficacy based on requirements elicited from the interviews that were conducted. OTnetic is a cyber security training program that utilizes a cyber range that allows trainees to learn about, and explore cybersecurity concepts by performing practical tasks and answering related questions.

The results from the lab experiment indicate that both the OTnetic training program and lecture-based training had a positive effect on learning outcome. The group using OTnetic had slightly better results on the post-test and reported that the learning experience was both motivating and engaging. Furthermore, participants responded more positively overall to this form of training, in contrast to the lecture-based training method, which received some positive and negative feedback. However, as stated in chapter 7, the limited sample size made the results from the lab experiment non-generalizable for the population. Additionally, due to time constraints, the participants for the lab experiment were not exclusively OT personnel working for the Norwegian energy sector. However, these participants had no background in IT, and were deemed sufficient candidates to participate in the lab experiment.

As stated in chapter 7, OTnetic was proven to be effective at training people with limited cyber security knowledge. The results of the thesis indicate that OTnetic is able to create a greater knowledge output than lectures. These findings are an important discovery, as they expose the value of using cyber range based training for teaching cyber security to OT-personnel, which is not commonly used today. However, due to the limitations discussed in chapter 7, more research would be beneficial in order to conclude whether OTnetic is well suited for providing cyber security training for OT personnel in the Norwegian energy sector.

To review, the results of this thesis indicates that cyber range based training can be an efficient and motivating method to teach OT-personnel in the Norwegian energy sector cyber security concepts. Furthermore, OTnetic outperforms lecture-based training when tested on two groups of participants lacking knowledge of cyber security and information technology. Participants using OTnetic also report greater motivation to complete training than the lecture group. This is likely due to practical nature of the training program, and inclusion of elements from game design. This facilitates active learning, which may be beneficial when aiming to produce long-term knowledge. As stated in the introduction of this thesis, there is gap, both in current research on effective cyber security training in the energy sector, and in the training currently given to these employees. We believe OTnetic can be a solution well suited to alleviate this research gap.

8.1 Reflection

During this thesis project, we have had the opportunity to get familiar with the design science research (DSR) approach. DSR allows for the creation of an artifact with purpose of solving the problem identified earlier in the same project. Therefore, this project has allowed us to identify and investigate the problem of training in the Norwegian energy sector, and create a solution to tackle this problem. Furthermore, as DSR utilizes both qualitative and quantitative methods for requirement elicitation and evaluation, we have gained valuable knowledge and experience tied to conducting interviews and lab experiments.

Additionally, we have gained great insight into the state of cybersecurity in critical infrastructure in Norway, what threats they face, and how training is conducted. Moreover, the motivational advantages of gamification have become increasingly apparent, which will aid us in the future development of OTnetic. Furthermore, we have had the opportunity to explore a variety of open source projects and tools. Setting up, modifying and testing these tools and programs has been a technical challenge from which we have gained valuable experience. Lastly, as the thesis was written in LaTeX, we have learned a lot about this language and the value it provides.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1).

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. *Computers & Security*, *29*(4), 432–445.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, *8*, 53–66.

Aldawood, H., & Skinner, G. (2019). Challenges of implementing training and awareness programs targeting cyber security social engineering. In *2019 cybersecurity and cyberforensics conference (ccc)* (pp. 111–117).

Apache Software Foundation. (2021). *Apache guacamole.* Retrieved 13.05.2021, from `https://guacamole.apache.org/`

Azam, N. (2017). Informasjonssikkerhetstilstanden i energiforsyningen. *Norges vassdrags-og energidirektorat, Oslo.*

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management*, *51*(1), 138–151.

Beuran, R., Pham, C., Tang, D., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2017). Cytrone: An integrated cybersecurity training framework.

Bigham, J., Gamez, D., & Lu, N. (2003). Safeguarding scada systems with anomaly detection. In *International workshop on mathematical methods, models, and architectures for computer network security* (pp. 171–182).

Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning cyber security through gamification. *Indian Journal of Science and Technology*, *8*(7), 642–649.

Cater-Steel, A., Toleman, M., & Rajaeian, M. M. (2019). Design science research in doctoral projects: An analysis of australian theses. *Journal of the Association for Information Systems*, *20*(12), 3.

CISA. (2020). *Critical infrastructure sectors.* Retrieved 05.10.2020, from `https://www.cisa.gov/critical-infrastructure-sectors`

Curtis, P. D., & Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. In *2015 ieee international symposium on technologies* *for homeland security (hst)* (pp. 1–6).

Dumitru, D., & Ion, T. (2019). Cybersecurity educational programs: Costs and benefits. *New Trends in Sustainable Business and Consumption*, 625.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667–4679.

Giuliano, V., & Formicola, V. (2019). Icsrange: A simulation-based cyber range platform for industrial control systems. *arXiv preprint arXiv:1909.01910*.

Hackathorn, J., Solomon, E. D., Blankmeyer, K. L., Tennial, R. E., & Garczynski, A. M. (2011). Learning by doing: An empirical study of active teaching techniques. *Journal of Effective Teaching*, *11*(2), 40–54.

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In *Design research in information systems* (pp. 9–22). Springer.

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75–105.

Hung, D. (2001). Theories of learning and computer-mediated instructional technologies. *Educational Media International*, *38*(4), 281–287.

Jaatun, M. G., Moe, M. E. G., & Istad, M. K. (2018). Cybersikkerhet i digitale transformatorstasjoner. forprosjekt. *SINTEF Rapport*.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). *What is the impact of successful cyberattacks target firms?* (Tech. Rep.). National Bureau of Economic Research.

Karjalainen, M. (2009). Review of is security training approaches: Implications for practice and research. *unpublished Licentiate thesis, University of Oulu, Finland*.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (is) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 3.

Kent State University. (2021). *Spss tutorials: Paired samples t test.* Retrieved 22.05.2021, from `https://libguides.library.kent.edu/SPSS/PairedSamplestTest`

Kick, J. (2014). *Cyber exercise playbook* (Tech. Rep.). MITRE CORP BEDFORD MA.

MacKinnon, L., Bacon, L., Gan, D., Loukas, G., Chadwick, D., & Frangiskatos, D. (2013). Cyber security countermeasures to combat cyber terrorism. In *Strategic intelligence management* (pp. 234–257). Elsevier.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). Byod: Security and privacy considerations. *It Professional*, *14*(5), 53–55.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. In *2012 ieee international conference on cyber technology in automation, control, and intelligent systems (cyber)* (pp. 256–262).

NC-Spectrum. (n.d.). *Om oss.* Retrieved from `https://www.nc-spectrum.no`

NIST. (2018). Cyber ranges. Retrieved 09.02.2021, from `https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf`

NSM. (2018). *Passordanbefalinger fra nasjonal sikkerhetsmyndighet.* Retrieved

14.04.2021, from https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet

NSM. (2019). *Råd og anbefalinger om passord.* Retrieved 14.04.2021, from https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. *The Electricity Journal*, *27*(2), 52–60.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards is security policy compliance. In *2007 40th annual hawaii international conference on system sciences (hicss'07)* (pp. 156b–156b).

Passord.net. (2021). *Passord generator.* Retrieved 14.05.2021, from https://passord.net/

Paton, D., & Jackson, D. (2002). Developing disaster management capability: an assessment centre approach. *Disaster Prevention and Management: An International Journal.*

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45–77.

Pipino, L. L., Lee, Y. W., & Wang, R. Y. (2002). Data quality assessment. *Communications of the ACM*, *45*(4), 211–218.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757–778.

PwC. (2014). Us cybercrime: Rising risks, reduced readiness key findings from the 2014 us state of cybercrime survey. Retrieved 11.11.2020, from https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Security.org. (2021). *How secure is my password?* Retrieved 14.05.2021, from https://www.security.org/how-secure-is-my-password/

Sinclair, H., Doyle, E. E., Johnston, D. M., & Paton, D. (2012). Assessing emergency management training and exercises. *Disaster Prevention and Management: An International Journal.*

Siponen, M., & Baskerville, R. L. (2018). Intervention effect rates as a path to research relevance: Information systems security example. *Journal of the Association for information Systems*, *19*(4).

Somarakis, I., Smyrlis, M., Fysarakis, K., & Spanoudakis, G. (2019). Model-driven cyber range training: A cyber security assurance perspective. In *Computer security* (pp. 172–184). Springer.

Spagnoletti, P., & Resca, A. (2008). The duality of information security management: fighting against predictable and unpredictable threats. *Journal of Information System Security*, *4*(3), 46–62.

Thuan, N. H., Drechsler, A., & Antunes, P. (2019). Construction of design science research questions. *Communications of the Association for Information Systems*, *44*(1), 20.

Unisys. (2014). *Critical infrastructure: Security preparedness and maturity.* Retrieved 11.11.2020, from `https://www.huntonak.com/files/upload/Unisys_Report_Critical_Infrastructure_Cybersecurity.pdf`

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). Feds: a framework for evaluation in design science research. *European journal of information systems*, *25*(1), 77–89.

Appendix A

Interview Guide for OT-personnel in the Norwegian Energy Sector (English)

The purpose of this interview is to gain a better understanding of OT-personnel's attitude towards information security, and establish what kind of training they receive in regards to cybersecurity. Before we begin, we would like to inform you that everything you say will not be tied to your name. Furthermore, if some of the questions are difficult to answer without sharing sensitive information, please let us know so we can avoid this.

A.1 Current Status of Training

1. Can you tell me what type of training OT-personnel receive in regards to cybersecurity?
2. How do think this training can be improved?
3. Do you feel like these training programs accurately reflect relevant cybersecurity issues?
4. Do you know if the company you work for has internal security policies for OT-systems or information security? (e.g. password rules, acceptable use policy)?
5. To what degree do you think other employees in the company comply with these rules and policies?

A.2 Attitudes Towards Information Security

Some people would argue that there is a gap between those who work with IT and OT, and what they are concerned with in regards to security, safety and work assignments.

1. Do you think your colleagues would agree with this statement?

2. Do you think employees not working with IT can affect the security level in your organization? Do you think most employees view security as a shared responsibility?

3. Do you think that employees in your organization have the knowledge and skills to assist in the work of securing the organization (e.g. detect phishing emails and errors in control systems/SCADA)?

4. Do you think that employees are aware that vulnerabilities may exist in operational systems that can be exploited by threat actors? Do you know if such vulnerabilities have been discovered and patched?

5. What do you think is the most critical threat in the "OT-world"? What kind of cyber attack do you believe would have the biggest impact on your organization and society?

6. Have you, or someone you know, experienced a security incident in your organization? How was this incident handled?

A.3 Opinions On Development of a New Training Program

During this master thesis, we will develop a training program made specifically for employees working with OT in the energy sector. To achieve the desired result, we need some help from the target audience. The product will most likely be made in the form of a framework or application built on principles of simulation and gamification, with various tasks and challenges.

1. Do you think other employees in the company you work for find IT and cybersecurity difficult and confusing?

2. How do you feel about completing a training program where you receive practical challenges and get to see cybersecurity from both sides (defense/attack)? Do you think other employees would be positive to this concept?

3. Is there anything specific you would like to learn more about in regards to cybersecurity, or something you think there is a need for in your company or the sector?

Appendix B

Interview Guide for Security Consulting Company (English)

B.1 Current Status of Training

1. Can you tell me about how cyber security training is given in the companies you work with?
2. What kind of training do you give to new employees who work with cybersecurity?
3. Does the company have a clear plans for roles and and responsibility in the occurrence of a cyber security related incident?
4. Do you feel like these training programs make a noticeable difference in terms of knowledge and preparedness?
5. Do you feel like these training programs left anything in regard to awareness about security related issues or technical preparedness?
6. Does NC-Spectrum offer any form of training for cyber security for your clients?
7. what kind of training have you experienced to be the most cost effective?

B.2 Security Requirements in the Energy Sector

1. Are there any specific or unique security requirements that are common for companies in the energy sector? (or in other critical infrastructure?)
2. Are there any requirements that differ, or do they mostly face the same security challenges?
3. Do these companies use substantially more resources on cybersecurity than other companies?

4. Can you tell me more about security issues or security incidents that are unique for companies in the energy sector? (i.e. in terms of operating cyber physical systems, responsibility for security, influence on society etc.)
5. Do you consider these companies as attractive targets for cyber criminals or other malicious actors?

B.3 Attack Simulation

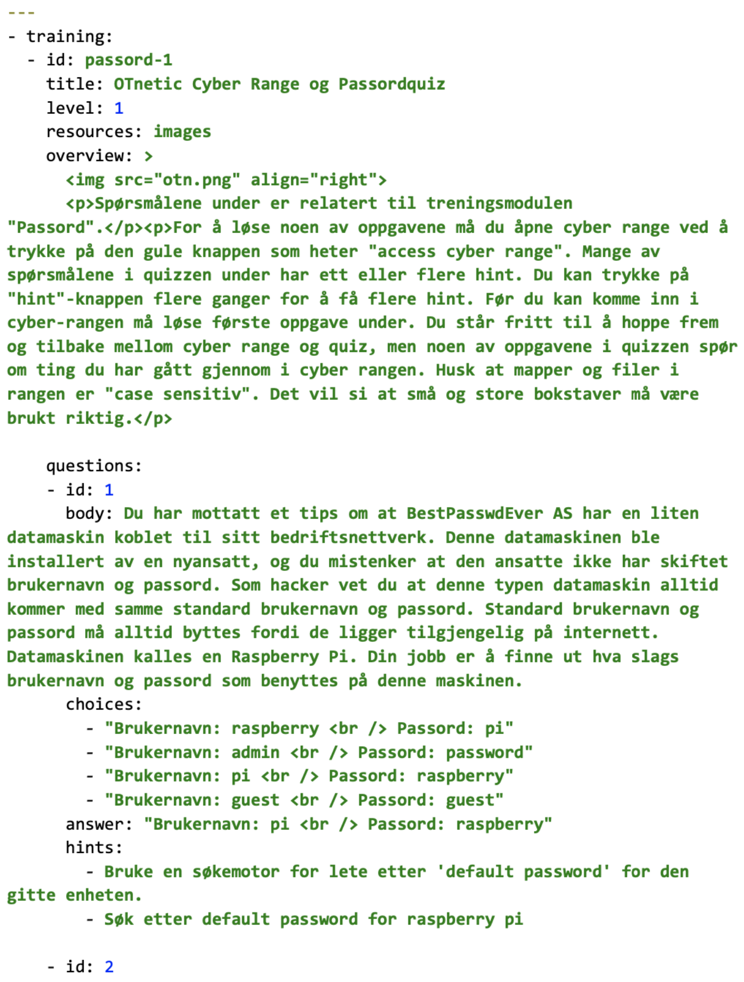
1. What type of attacks are most common in your company or your clients companies? What kinds of attacks have the greatest impact?
2. Do you utilize cyber ranges or other forms of red/blue team training (such as penetration testing)?
3. Do you think that simulating specific attack types in a controlled environment for security professionals in their company could improve the abilities of the participants? (make them better prepared for such attacks in a realistic setting)
4. What do you think would be challenging with such a training program?
5. what do you think would be beneficial with implementing such a training program?

B.4 Use of Existing Training Frameworks

1. Do you use any existing frameworks for training that are relevant for cyber security? (If yes: what?)
2. How have you customized these frameworks to fit your unique needs and security requirements?
3. What are your current focus areas in the frameworks and programs you use? (i.e. detection, prevention, risk assessment etc.)

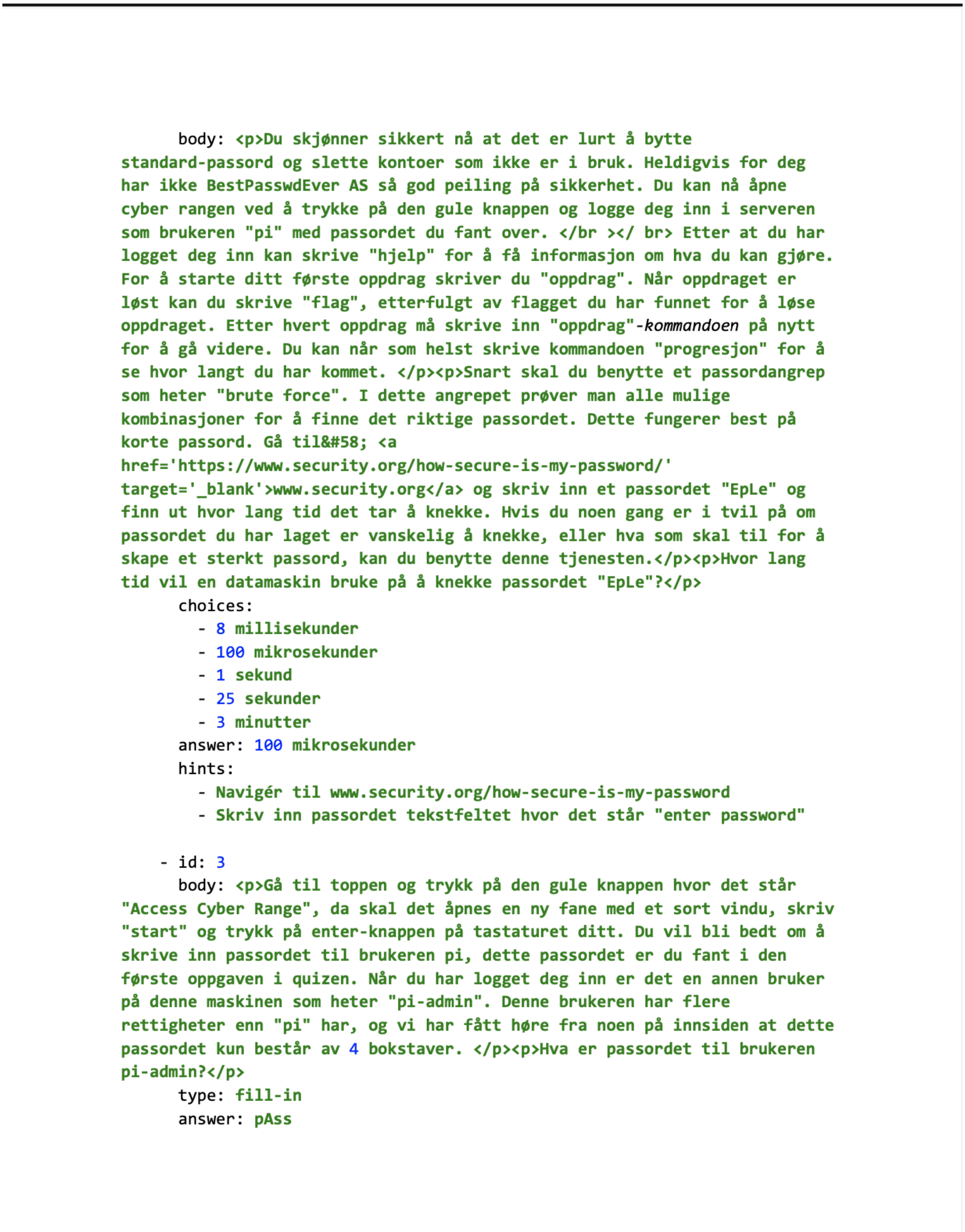
Appendix C

OTnetic Password Quiz



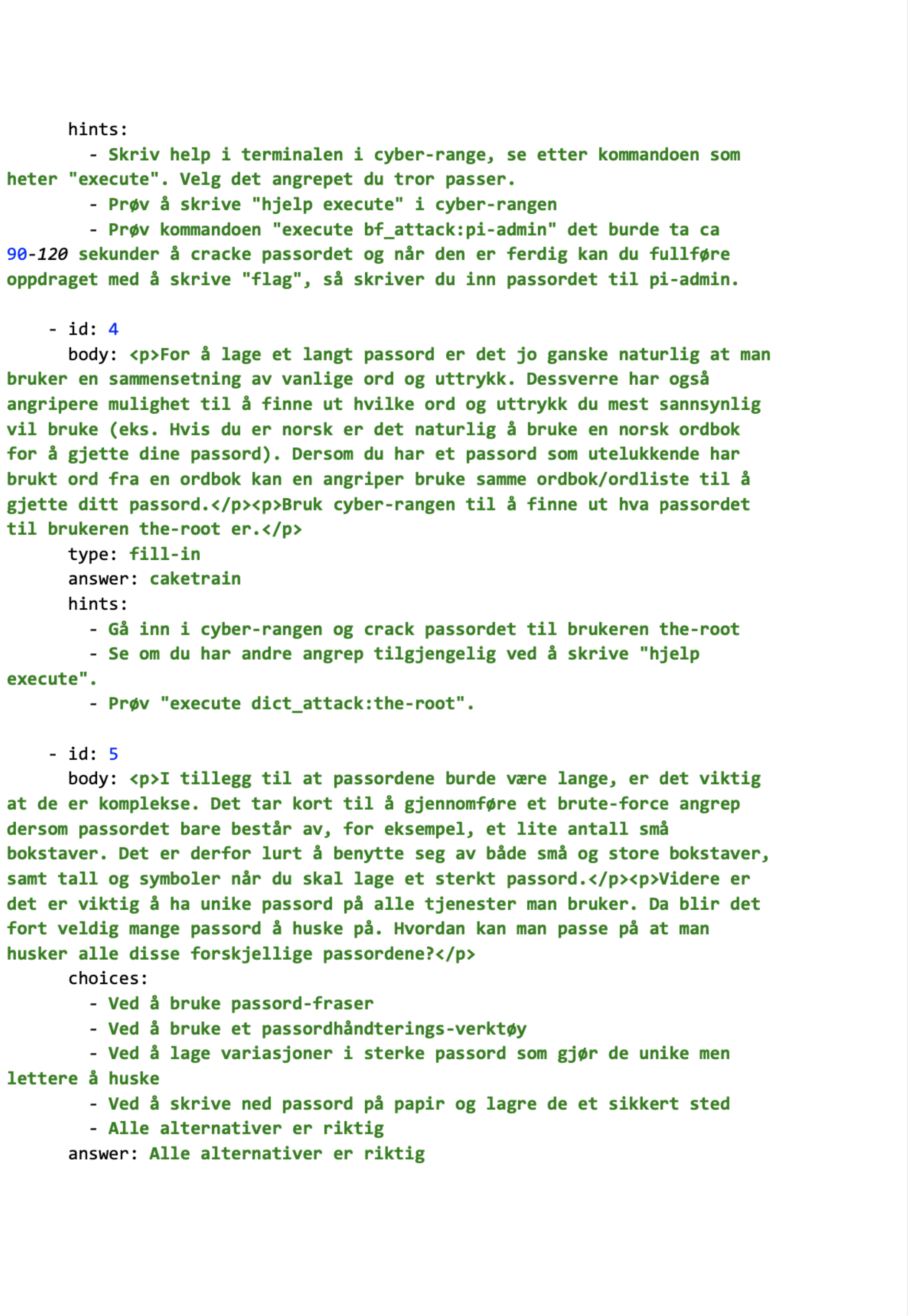
```
---
- training:
  - id: passord-1
    title: OTnetic Cyber Range og Passordquiz
    level: 1
    resources: images
    overview: >
      <img src="otn.png" align="right">
      <p>Spørsmålene under er relatert til treningsmodulen
"Passord".</p><p>For å løse noen av oppgavene må du åpne cyber range ved å
trykke på den gule knappen som heter "access cyber range". Mange av
spørsmålene i quizzen under har ett eller flere hint. Du kan trykke på
"hint"-knappen flere ganger for å få flere hint. Før du kan komme inn i
cyber-rangen må løse første oppgave under. Du står fritt til å hoppe frem
og tilbake mellom cyber range og quiz, men noen av oppgavene i quizzen spør
om ting du har gått gjennom i cyber rangen. Husk at mapper og filer i
rangen er "case sensitiv". Det vil si at små og store bokstaver må være
brukt riktig.</p>

    questions:
    - id: 1
      body: Du har mottatt et tips om at BestPasswdEver AS har en liten
datamaskin koblet til sitt bedriftsnettverk. Denne datamaskinen ble
installert av en nyansatt, og du mistenker at den ansatte ikke har skiftet
brukernavn og passord. Som hacker vet du at denne typen datamaskin alltid
kommer med samme standard brukernavn og passord. Standard brukernavn og
passord må alltid byttes fordi de ligger tilgjengelig på internett.
Datamaskinen kalles en Raspberry Pi. Din jobb er å finne ut hva slags
brukernavn og passord som benyttes på denne maskinen.
      choices:
        - "Brukernavn: raspberry <br /> Passord: pi"
        - "Brukernavn: admin <br /> Passord: password"
        - "Brukernavn: pi <br /> Passord: raspberry"
        - "Brukernavn: guest <br /> Passord: guest"
      answer: "Brukernavn: pi <br /> Passord: raspberry"
      hints:
        - Bruke en søkemotor for lete etter 'default password' for den
gitte enheten.
        - Søk etter default password for raspberry pi

    - id: 2
```

Figure C.1: Cyber Range Quiz YAML 1



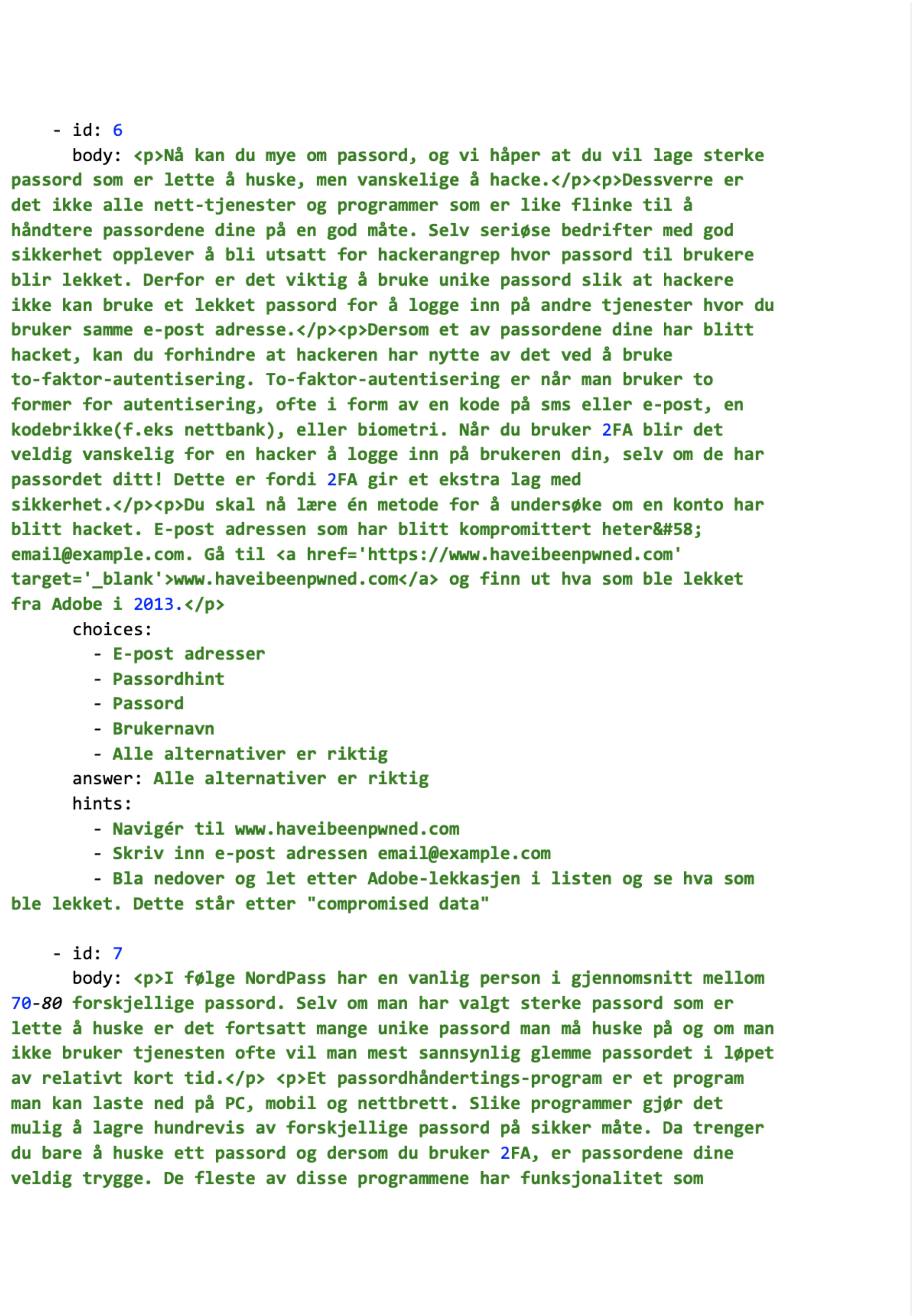
```
      body: <p>Du skjønner sikkert nå at det er lurt å bytte
standard-passord og slette kontoer som ikke er i bruk. Heldigvis for deg
har ikke BestPasswdEver AS så god peiling på sikkerhet. Du kan nå åpne
cyber rangen ved å trykke på den gule knappen og logge deg inn i serveren
som brukeren "pi" med passordet du fant over. </br ></ br> Etter at du har
logget deg inn kan skrive "hjelp" for å få informasjon om hva du kan gjøre.
For å starte ditt første oppdrag skriver du "oppdrag". Når oppdraget er
løst kan du skrive "flag", etterfulgt av flagget du har funnet for å løse
oppdraget. Etter hvert oppdrag må skrive inn "oppdrag"-kommandoen på nytt
for å gå videre. Du kan når som helst skrive kommandoen "progresjon" for å
se hvor langt du har kommet. </p><p>Snart skal du benytte et passordangrep
som heter "brute force". I dette angrepet prøver man alle mulige
kombinasjoner for å finne det riktige passordet. Dette fungerer best på
korte passord. Gå til&#58; <a
href='https://www.security.org/how-secure-is-my-password/'
target='_blank'>www.security.org</a> og skriv inn et passordet "EpLe" og
finn ut hvor lang tid det tar å knekke. Hvis du noen gang er i tvil på om
passordet du har laget er vanskelig å knekke, eller hva som skal til for å
skape et sterkt passord, kan du benytte denne tjenesten.</p><p>Hvor lang
tid vil en datamaskin bruke på å knekke passordet "EpLe"?</p>
      choices:
        - 8 millisekunder
        - 100 mikrosekunder
        - 1 sekund
        - 25 sekunder
        - 3 minutter
      answer: 100 mikrosekunder
      hints:
        - Navigér til www.security.org/how-secure-is-my-password
        - Skriv inn passordet tekstfeltet hvor det står "enter password"

    - id: 3
      body: <p>Gå til toppen og trykk på den gule knappen hvor det står
"Access Cyber Range", da skal det åpnes en ny fane med et sort vindu, skriv
"start" og trykk på enter-knappen på tastaturet ditt. Du vil bli bedt om å
skrive inn passordet til brukeren pi, dette passordet er du fant i den
første oppgaven i quizen. Når du har logget deg inn er det en annen bruker
på denne maskinen som heter "pi-admin". Denne brukeren har flere
rettigheter enn "pi" har, og vi har fått høre fra noen på innsiden at dette
passordet kun består av 4 bokstaver. </p><p>Hva er passordet til brukeren
pi-admin?</p>
      type: fill-in
      answer: pAss
```

Figure C.2: Cyber Range Quiz YAML 2



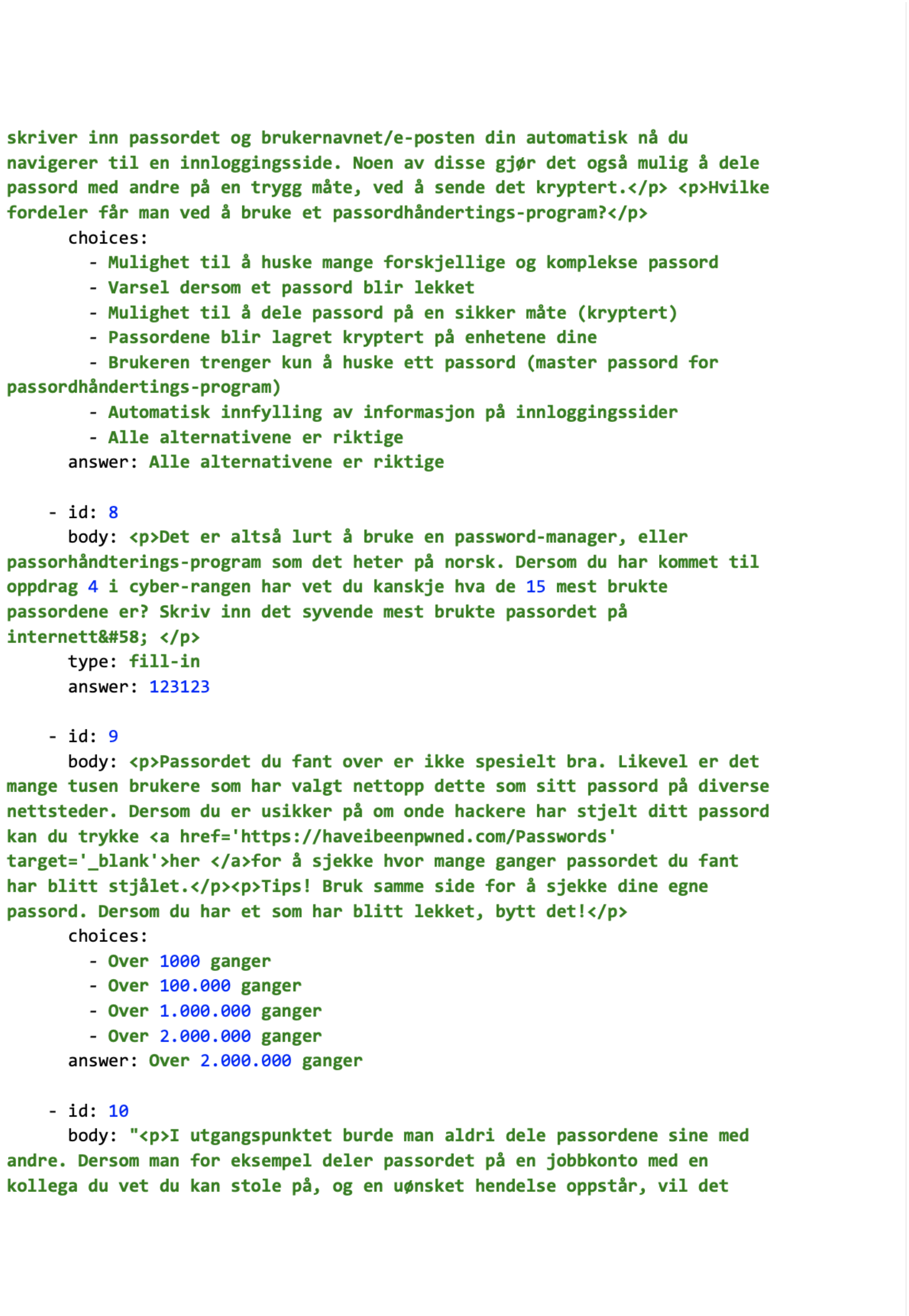
```
      hints:
        - Skriv help i terminalen i cyber-range, se etter kommandoen som
heter "execute". Velg det angrepet du tror passer.
        - Prøv å skrive "hjelp execute" i cyber-rangen
        - Prøv kommandoen "execute bf_attack:pi-admin" det burde ta ca
90-120 sekunder å cracke passordet og når den er ferdig kan du fullføre
oppdraget med å skrive "flag", så skriver du inn passordet til pi-admin.

    - id: 4
      body: <p>For å lage et langt passord er det jo ganske naturlig at man
bruker en sammensetning av vanlige ord og uttrykk. Dessverre har også
angripere mulighet til å finne ut hvilke ord og uttrykk du mest sannsynlig
vil bruke (eks. Hvis du er norsk er det naturlig å bruke en norsk ordbok
for å gjette dine passord). Dersom du har et passord som utelukkende har
brukt ord fra en ordbok kan en angriper bruke samme ordbok/ordliste til å
gjette ditt passord.</p><p>Bruk cyber-rangen til å finne ut hva passordet
til brukeren the-root er.</p>
      type: fill-in
      answer: caketrain
      hints:
        - Gå inn i cyber-rangen og crack passordet til brukeren the-root
        - Se om du har andre angrep tilgjengelig ved å skrive "hjelp
execute".
        - Prøv "execute dict_attack:the-root".

    - id: 5
      body: <p>I tillegg til at passordene burde være lange, er det viktig
at de er komplekse. Det tar kort til å gjennomføre et brute-force angrep
dersom passordet bare består av, for eksempel, et lite antall små
bokstaver. Det er derfor lurt å benytte seg av både små og store bokstaver,
samt tall og symboler når du skal lage et sterkt passord.</p><p>Videre er
det er viktig å ha unike passord på alle tjenester man bruker. Da blir det
fort veldig mange passord å huske på. Hvordan kan man passe på at man
husker alle disse forskjellige passordene?</p>
      choices:
        - Ved å bruke passord-fraser
        - Ved å bruke et passordhåndterings-verktøy
        - Ved å lage variasjoner i sterke passord som gjør de unike men
lettere å huske
        - Ved å skrive ned passord på papir og lagre de et sikkert sted
        - Alle alternativer er riktig
      answer: Alle alternativer er riktig
```

Figure C.3: Cyber Range Quiz YAML 3



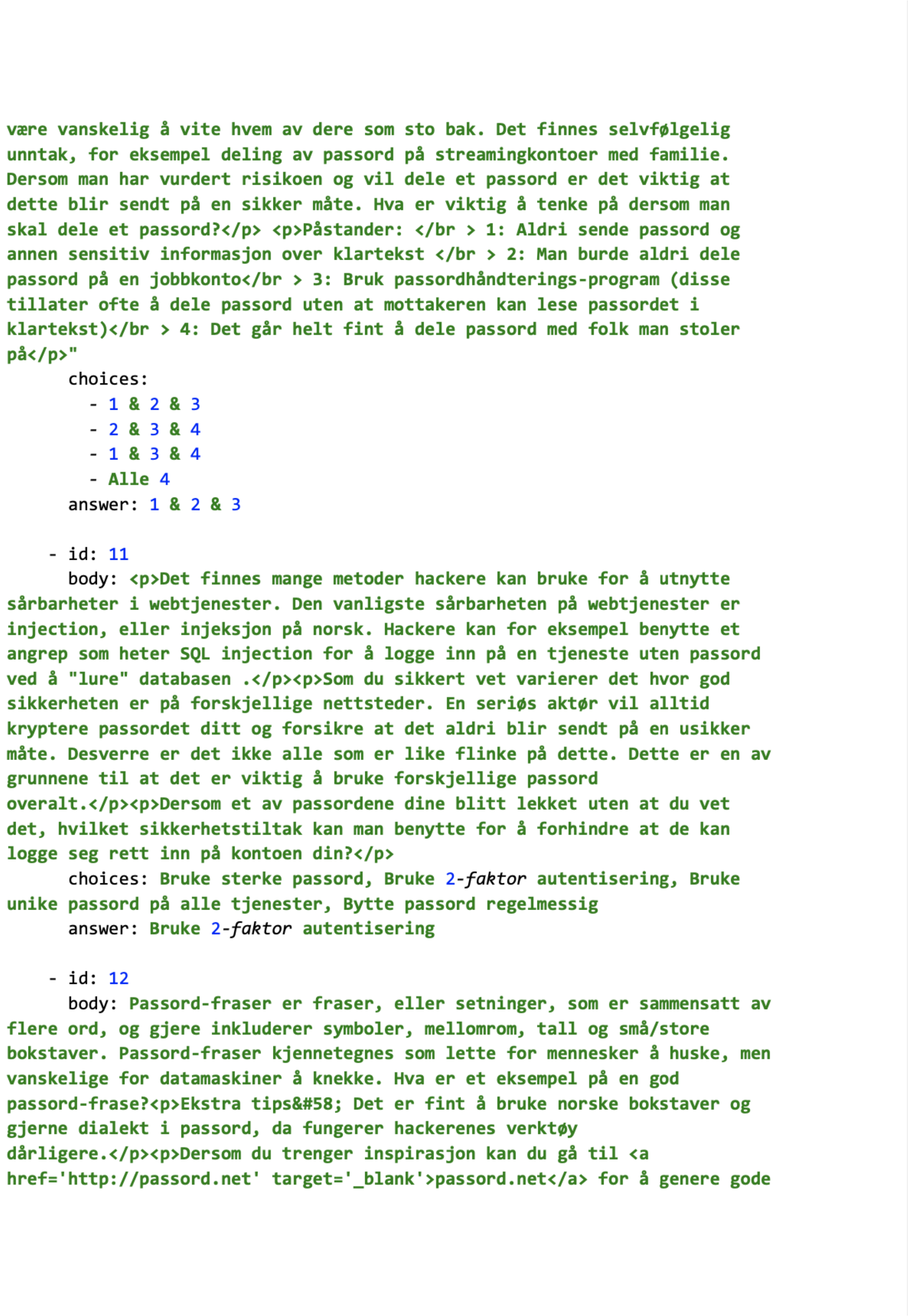
```
    - id: 6
      body: <p>Nå kan du mye om passord, og vi håper at du vil lage sterke
passord som er lette å huske, men vanskelige å hacke.</p><p>Dessverre er
det ikke alle nett-tjenester og programmer som er like flinke til å
håndtere passordene dine på en god måte. Selv seriøse bedrifter med god
sikkerhet opplever å bli utsatt for hackerangrep hvor passord til brukere
blir lekket. Derfor er det viktig å bruke unike passord slik at hackere
ikke kan bruke et lekket passord for å logge inn på andre tjenester hvor du
bruker samme e-post adresse.</p><p>Dersom et av passordene dine har blitt
hacket, kan du forhindre at hackeren har nytte av det ved å bruke
to-faktor-autentisering. To-faktor-autentisering er når man bruker to
former for autentisering, ofte i form av en kode på sms eller e-post, en
kodebrikke(f.eks nettbank), eller biometri. Når du bruker 2FA blir det
veldig vanskelig for en hacker å logge inn på brukeren din, selv om de har
passordet ditt! Dette er fordi 2FA gir et ekstra lag med
sikkerhet.</p><p>Du skal nå lære én metode for å undersøke om en konto har
blitt hacket. E-post adressen som har blitt kompromittert heter&#58;
email@example.com. Gå til <a href='https://www.haveibeenpwned.com'
target='_blank'>www.haveibeenpwned.com</a> og finn ut hva som ble lekket
fra Adobe i 2013.</p>
      choices:
        - E-post adresser
        - Passordhint
        - Passord
        - Brukernavn
        - Alle alternativer er riktig
      answer: Alle alternativer er riktig
      hints:
        - Navigér til www.haveibeenpwned.com
        - Skriv inn e-post adressen email@example.com
        - Bla nedover og let etter Adobe-lekkasjen i listen og se hva som
ble lekket. Dette står etter "compromised data"

    - id: 7
      body: <p>I følge NordPass har en vanlig person i gjennomsnitt mellom
70-80 forskjellige passord. Selv om man har valgt sterke passord som er
lette å huske er det fortsatt mange unike passord man må huske på og om man
ikke bruker tjenesten ofte vil man mest sannsynlig glemme passordet i løpet
av relativt kort tid.</p> <p>Et passordhåndertings-program er et program
man kan laste ned på PC, mobil og nettbrett. Slike programmer gjør det
mulig å lagre hundrevis av forskjellige passord på sikker måte. Da trenger
du bare å huske ett passord og dersom du bruker 2FA, er passordene dine
veldig trygge. De fleste av disse programmene har funksjonalitet som
```

Figure C.4: Cyber Range Quiz YAML 4



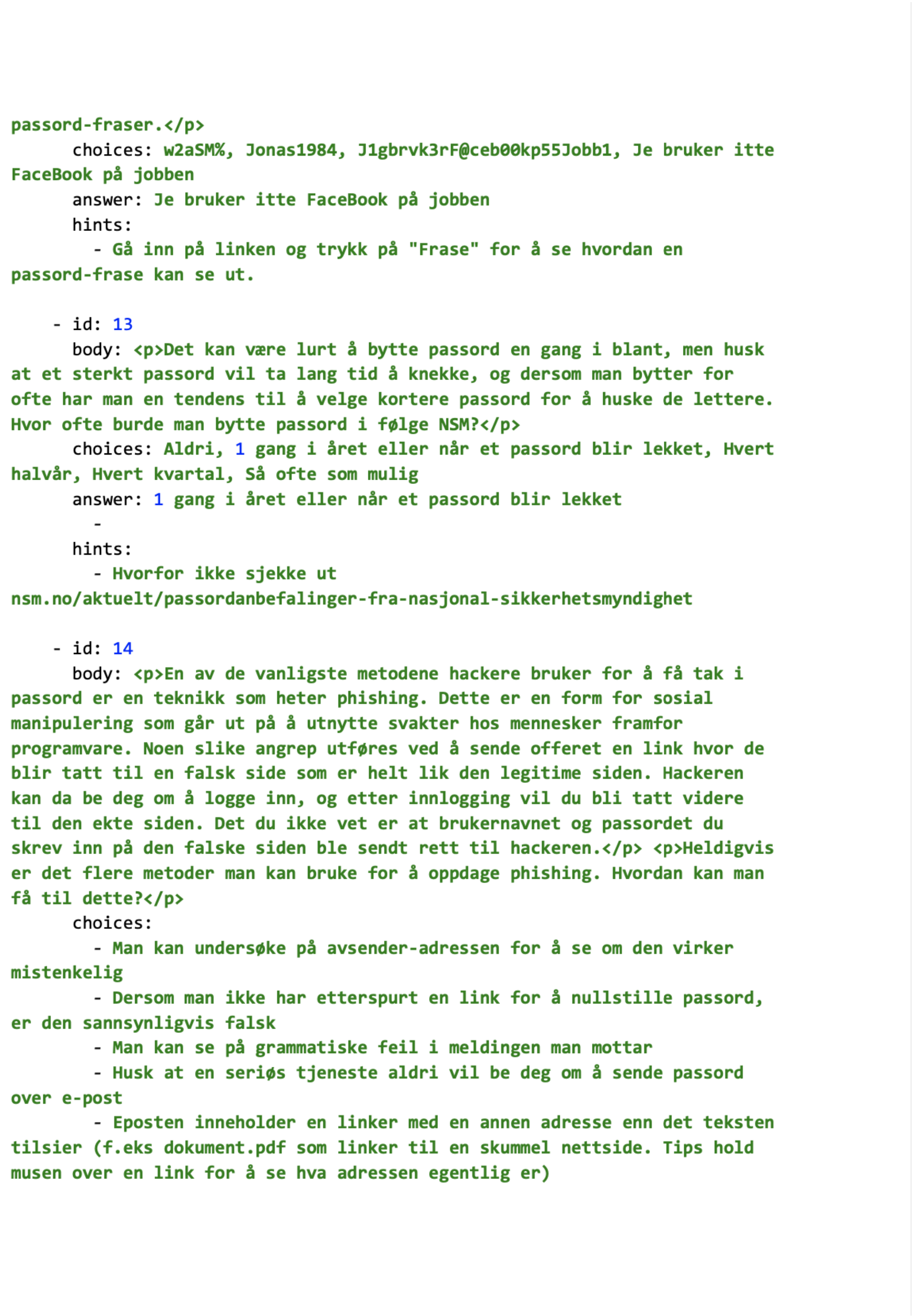
```
skriver inn passordet og brukernavnet/e-posten din automatisk nå du
navigerer til en innloggingsside. Noen av disse gjør det også mulig å dele
passord med andre på en trygg måte, ved å sende det kryptert.</p> <p>Hvilke
fordeler får man ved å bruke et passordhåndertings-program?</p>
      choices:
        - Mulighet til å huske mange forskjellige og komplekse passord
        - Varsel dersom et passord blir lekket
        - Mulighet til å dele passord på en sikker måte (kryptert)
        - Passordene blir lagret kryptert på enhetene dine
        - Brukeren trenger kun å huske ett passord (master passord for
passordhåndertings-program)
        - Automatisk innfylling av informasjon på innloggingssider
        - Alle alternativene er riktige
      answer: Alle alternativene er riktige

    - id: 8
      body: <p>Det er altså lurt å bruke en password-manager, eller
passorhåndtering-program som det heter på norsk. Dersom du har kommet til
oppdrag 4 i cyber-rangen har vet du kanskje hva de 15 mest brukte
passordene er? Skriv inn det syvende mest brukte passordet på
internett&#58; </p>
      type: fill-in
      answer: 123123

    - id: 9
      body: <p>Passordet du fant over er ikke spesielt bra. Likevel er det
mange tusen brukere som har valgt nettopp dette som sitt passord på diverse
nettsteder. Dersom du er usikker på om onde hackere har stjelt ditt passord
kan du trykke <a href='https://haveibeenpwned.com/Passwords'
target='_blank'>her </a>for å sjekke hvor mange ganger passordet du fant
har blitt stjålet.</p><p>Tips! Bruk samme side for å sjekke dine egne
passord. Dersom du har et som har blitt lekket, bytt det!</p>
      choices:
        - Over 1000 ganger
        - Over 100.000 ganger
        - Over 1.000.000 ganger
        - Over 2.000.000 ganger
      answer: Over 2.000.000 ganger

    - id: 10
      body: "<p>I utgangspunktet burde man aldri dele passordene sine med
andre. Dersom man for eksempel deler passordet på en jobbkonto med en
kollega du vet du kan stole på, og en uønsket hendelse oppstår, vil det
```

Figure C.5: Cyber Range Quiz YAML 5



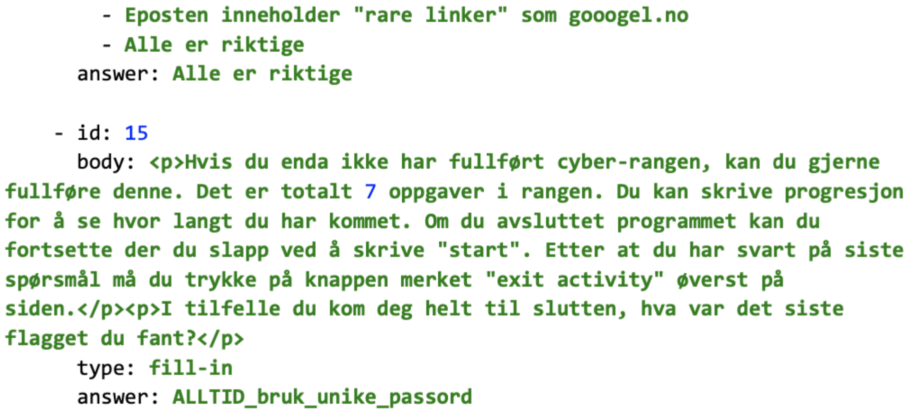
```
være vanskelig å vite hvem av dere som sto bak. Det finnes selvfølgelig
unntak, for eksempel deling av passord på streamingkontoer med familie.
Dersom man har vurdert risikoen og vil dele et passord er det viktig at
dette blir sendt på en sikker måte. Hva er viktig å tenke på dersom man
skal dele et passord?</p> <p>Påstander: </br > 1: Aldri sende passord og
annen sensitiv informasjon over klartekst </br > 2: Man burde aldri dele
passord på en jobbkonto</br > 3: Bruk passordhåndterings-program (disse
tillater ofte å dele passord uten at mottakeren kan lese passordet i
klartekst)</br > 4: Det går helt fint å dele passord med folk man stoler
på</p>"
      choices:
        - 1 & 2 & 3
        - 2 & 3 & 4
        - 1 & 3 & 4
        - Alle 4
      answer: 1 & 2 & 3

    - id: 11
      body: <p>Det finnes mange metoder hackere kan bruke for å utnytte
sårbarheter i webtjenester. Den vanligste sårbarheten på webtjenester er
injection, eller injeksjon på norsk. Hackere kan for eksempel benytte et
angrep som heter SQL injection for å logge inn på en tjeneste uten passord
ved å "lure" databasen .</p><p>Som du sikkert vet varierer det hvor god
sikkerheten er på forskjellige nettsteder. En seriøs aktør vil alltid
kryptere passordet ditt og forsikre at det aldri blir sendt på en usikker
måte. Desverre er det ikke alle som er like flinke på dette. Dette er en av
grunnene til at det er viktig å bruke forskjellige passord
overalt.</p><p>Dersom et av passordene dine blitt lekket uten at du vet
det, hvilket sikkerhetstiltak kan man benytte for å forhindre at de kan
logge seg rett inn på kontoen din?</p>
      choices: Bruke sterke passord, Bruke 2-faktor autentisering, Bruke
unike passord på alle tjenester, Bytte passord regelmessig
      answer: Bruke 2-faktor autentisering

    - id: 12
      body: Passord-fraser er fraser, eller setninger, som er sammensatt av
flere ord, og gjere inkluderer symboler, mellomrom, tall og små/store
bokstaver. Passord-fraser kjennetegnes som lette for mennesker å huske, men
vanskelige for datamaskiner å knekke. Hva er et eksempel på en god
passord-frase?<p>Ekstra tips&#58; Det er fint å bruke norske bokstaver og
gjerne dialekt i passord, da fungerer hackerenes verktøy
dårligere.</p><p>Dersom du trenger inspirasjon kan du gå til <a
href='http://passord.net' target='_blank'>passord.net</a> for å genere gode
```

Figure C.6: Cyber Range Quiz YAML 6



```
passord-fraser.</p>
      choices: w2aSM%, Jonas1984, J1gbrvk3rF@ceb00kp55Jobb1, Je bruker itte
FaceBook på jobben
      answer: Je bruker itte FaceBook på jobben
      hints:
        - Gå inn på linken og trykk på "Frase" for å se hvordan en
passord-frase kan se ut.

    - id: 13
      body: <p>Det kan være lurt å bytte passord en gang i blant, men husk
at et sterkt passord vil ta lang tid å knekke, og dersom man bytter for
ofte har man en tendens til å velge kortere passord for å huske de lettere.
Hvor ofte burde man bytte passord i følge NSM?</p>
      choices: Aldri, 1 gang i året eller når et passord blir lekket, Hvert
halvår, Hvert kvartal, Så ofte som mulig
      answer: 1 gang i året eller når et passord blir lekket
        -
      hints:
        - Hvorfor ikke sjekke ut
nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet

    - id: 14
      body: <p>En av de vanligste metodene hackere bruker for å få tak i
passord er en teknikk som heter phishing. Dette er en form for sosial
manipulering som går ut på å utnytte svakter hos mennesker framfor
programvare. Noen slike angrep utføres ved å sende offeret en link hvor de
blir tatt til en falsk side som er helt lik den legitime siden. Hackeren
kan da be deg om å logge inn, og etter innlogging vil du bli tatt videre
til den ekte siden. Det du ikke vet er at brukernavnet og passordet du
skrev inn på den falske siden ble sendt rett til hackeren.</p> <p>Heldigvis
er det flere metoder man kan bruke for å oppdage phishing. Hvordan kan man
få til dette?</p>
      choices:
        - Man kan undersøke på avsender-adressen for å se om den virker
mistenkelig
        - Dersom man ikke har etterspurt en link for å nullstille passord,
er den sannsynligvis falsk
        - Man kan se på grammatiske feil i meldingen man mottar
        - Husk at en seriøs tjeneste aldri vil be deg om å sende passord
over e-post
        - Eposten inneholder en linker med en annen adresse enn det teksten
tilsier (f.eks dokument.pdf som linker til en skummel nettside. Tips hold
musen over en link for å se hva adressen egentlig er)
```

Figure C.7: Cyber Range Quiz YAML 7

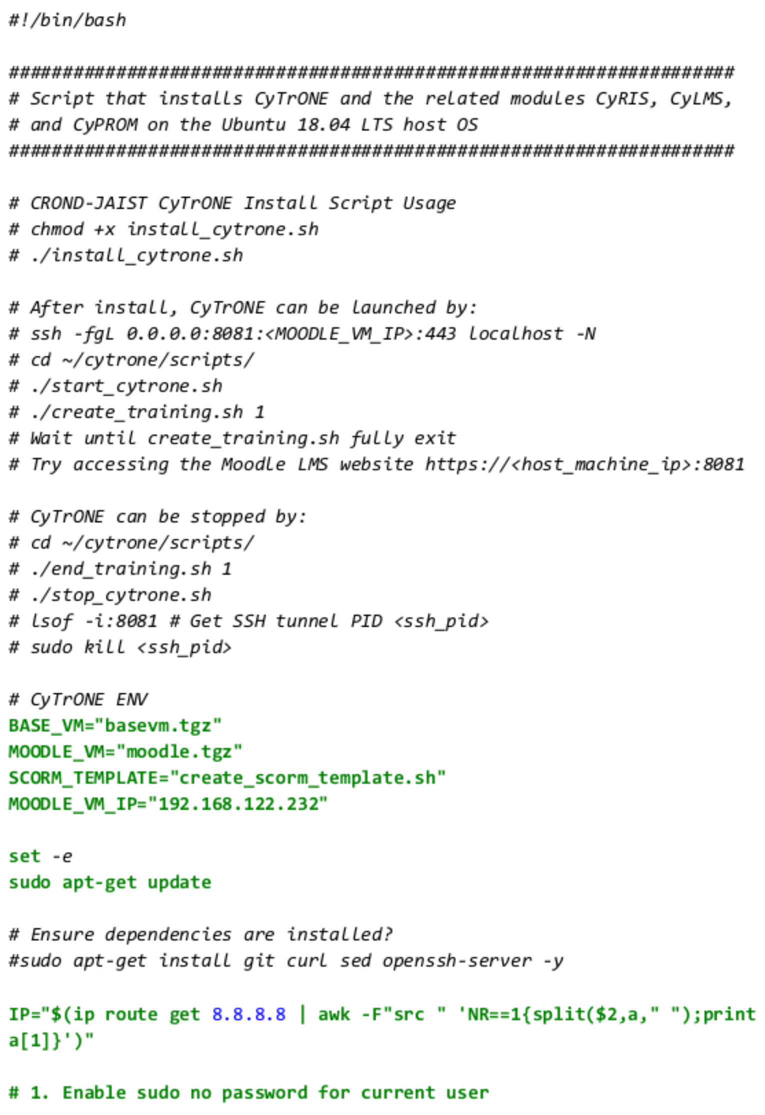


```
        - Eposten inneholder "rare linker" som gooogel.no
        - Alle er riktige
      answer: Alle er riktige

    - id: 15
      body: <p>Hvis du enda ikke har fullført cyber-rangen, kan du gjerne
fullføre denne. Det er totalt 7 oppgaver i rangen. Du kan skrive progresjon
for å se hvor langt du har kommet. Om du avsluttet programmet kan du
fortsette der du slapp ved å skrive "start". Etter at du har svart på siste
spørsmål må du trykke på knappen merket "exit activity" øverst på
siden.</p><p>I tilfelle du kom deg helt til slutten, hva var det siste
flagget du fant?</p>
      type: fill-in
      answer: ALLTID_bruk_unike_passord
```

Figure C.8: Cyber Range Quiz YAML 8

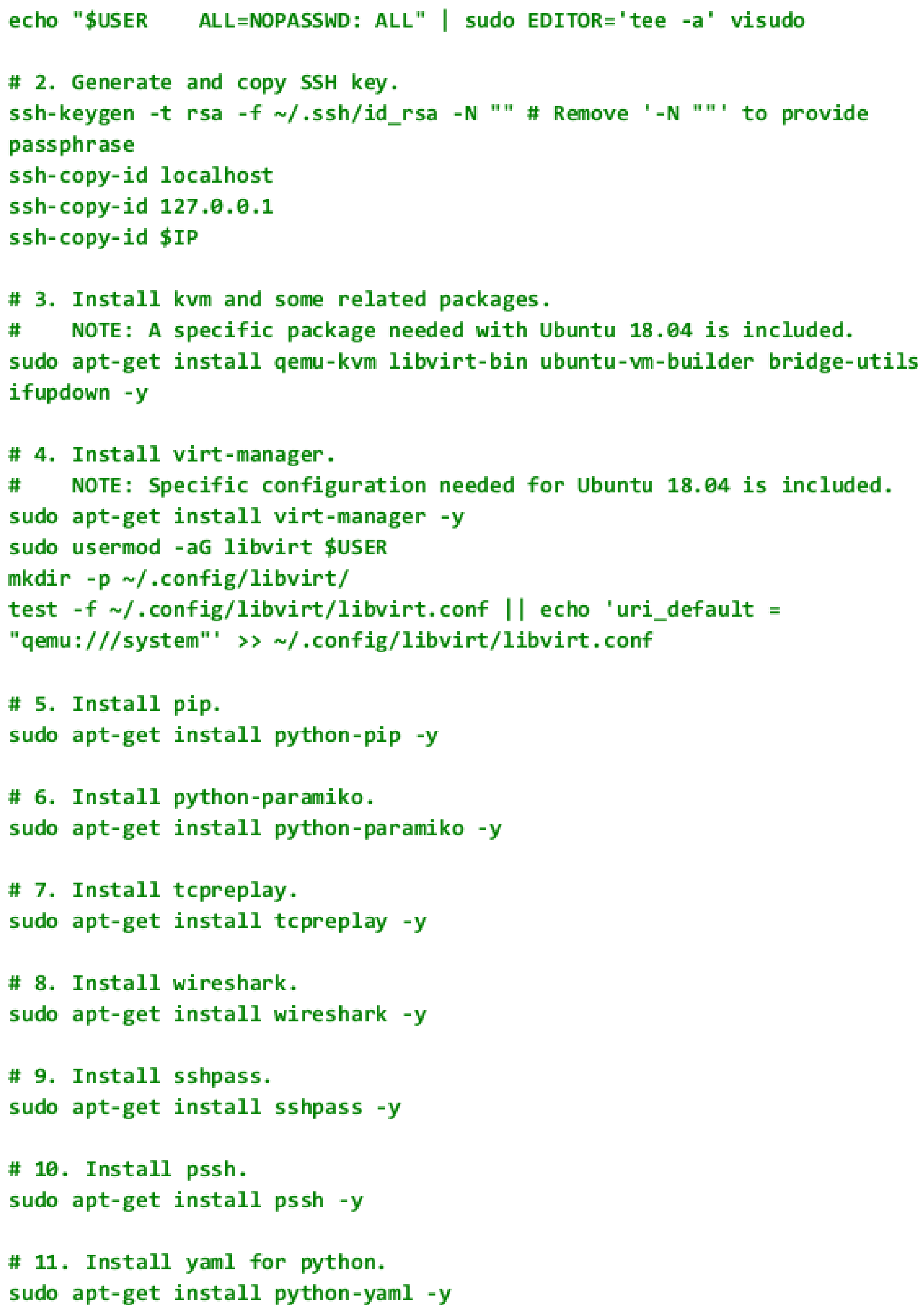
Appendix D

CyTrONE Installation Script



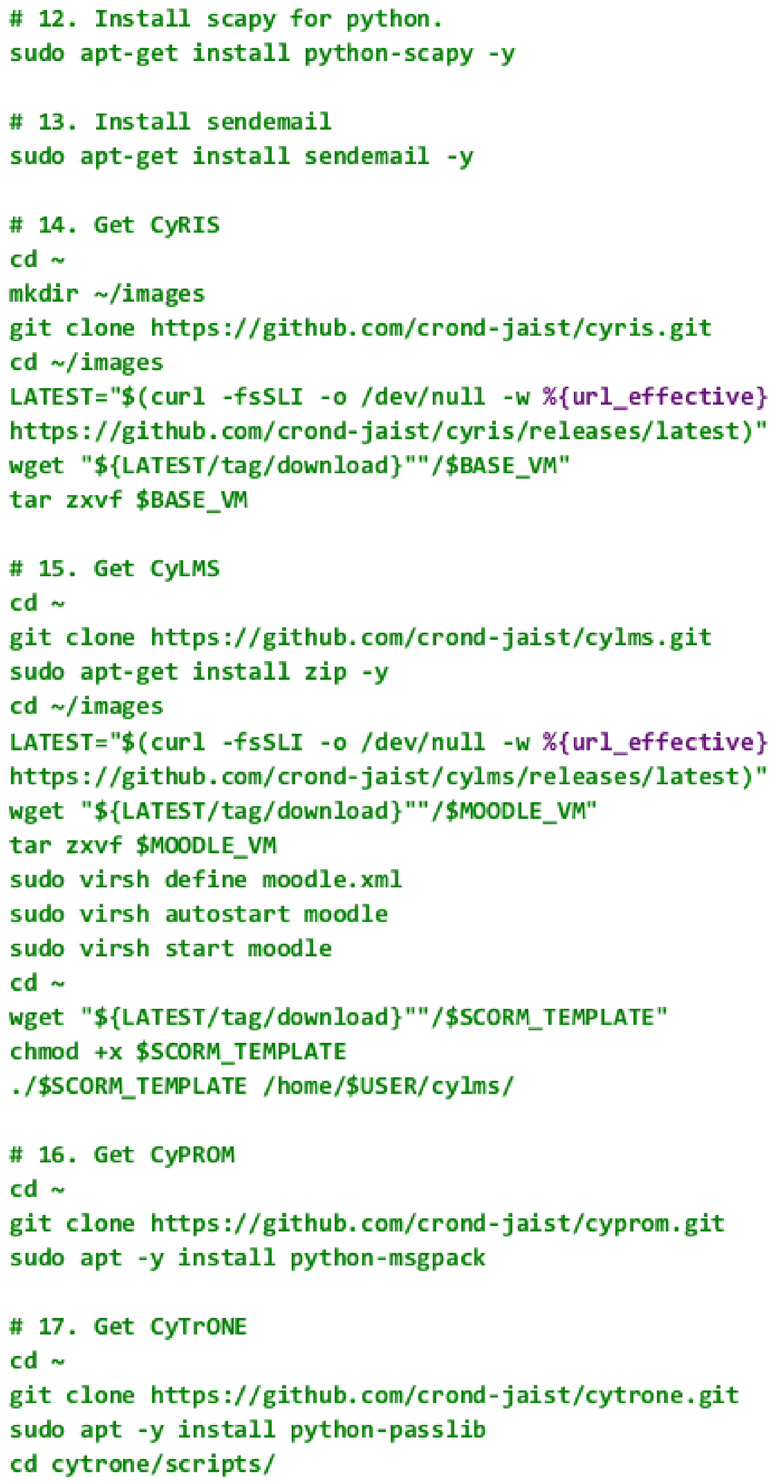
```
#!/bin/bash

####################################################################
# Script that installs CyTrONE and the related modules CyRIS, CyLMS,
# and CyPROM on the Ubuntu 18.04 LTS host OS
####################################################################

# CROND-JAIST CyTrONE Install Script Usage
# chmod +x install_cytrone.sh
# ./install_cytrone.sh

# After install, CyTrONE can be launched by:
# ssh -fgL 0.0.0.0:8081:<MOODLE_VM_IP>:443 localhost -N
# cd ~/cytrone/scripts/
# ./start_cytrone.sh
# ./create_training.sh 1
# Wait until create_training.sh fully exit
# Try accessing the Moodle LMS website https://<host_machine_ip>:8081

# CyTrONE can be stopped by:
# cd ~/cytrone/scripts/
# ./end_training.sh 1
# ./stop_cytrone.sh
# lsof -i:8081 # Get SSH tunnel PID <ssh_pid>
# sudo kill <ssh_pid>

# CyTrONE ENV
BASE_VM="basevm.tgz"
MOODLE_VM="moodle.tgz"
SCORM_TEMPLATE="create_scorm_template.sh"
MOODLE_VM_IP="192.168.122.232"

set -e
sudo apt-get update

# Ensure dependencies are installed?
#sudo apt-get install git curl sed openssh-server -y

IP="$(ip route get 8.8.8.8 | awk -F"src " 'NR==1{split($2,a," ");print
a[1]}')"

# 1. Enable sudo no password for current user
```

Figure D.1: CyTrONE Installation Script 1



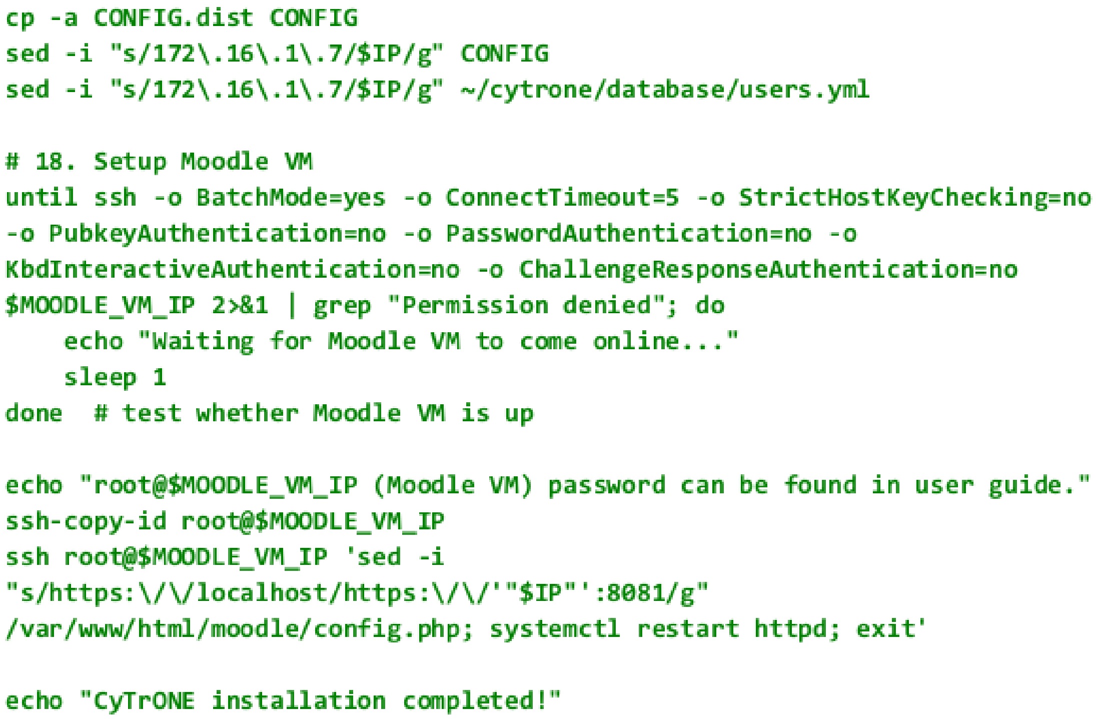
```
echo "$USER    ALL=NOPASSWD: ALL" | sudo EDITOR='tee -a' visudo

# 2. Generate and copy SSH key.
ssh-keygen -t rsa -f ~/.ssh/id_rsa -N "" # Remove '-N ""' to provide
passphrase
ssh-copy-id localhost
ssh-copy-id 127.0.0.1
ssh-copy-id $IP

# 3. Install kvm and some related packages.
#    NOTE: A specific package needed with Ubuntu 18.04 is included.
sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils
ifupdown -y

# 4. Install virt-manager.
#    NOTE: Specific configuration needed for Ubuntu 18.04 is included.
sudo apt-get install virt-manager -y
sudo usermod -aG libvirt $USER
mkdir -p ~/.config/libvirt/
test -f ~/.config/libvirt/libvirt.conf || echo 'uri_default =
"qemu:///system"' >> ~/.config/libvirt/libvirt.conf

# 5. Install pip.
sudo apt-get install python-pip -y

# 6. Install python-paramiko.
sudo apt-get install python-paramiko -y

# 7. Install tcpreplay.
sudo apt-get install tcpreplay -y

# 8. Install wireshark.
sudo apt-get install wireshark -y

# 9. Install sshpass.
sudo apt-get install sshpass -y

# 10. Install pssh.
sudo apt-get install pssh -y

# 11. Install yaml for python.
sudo apt-get install python-yaml -y
```

Figure D.2: CyTrONE Installation Script 2



```
# 12. Install scapy for python.
sudo apt-get install python-scapy -y

# 13. Install sendemail
sudo apt-get install sendemail -y

# 14. Get CyRIS
cd ~
mkdir ~/images
git clone https://github.com/crond-jaist/cyris.git
cd ~/images
LATEST="$(curl -fsSLI -o /dev/null -w %{url_effective}
https://github.com/crond-jaist/cyris/releases/latest)"
wget "${LATEST/tag/download}""/$BASE_VM"
tar zxvf $BASE_VM

# 15. Get CyLMS
cd ~
git clone https://github.com/crond-jaist/cylms.git
sudo apt-get install zip -y
cd ~/images
LATEST="$(curl -fsSLI -o /dev/null -w %{url_effective}
https://github.com/crond-jaist/cylms/releases/latest)"
wget "${LATEST/tag/download}""/$MOODLE_VM"
tar zxvf $MOODLE_VM
sudo virsh define moodle.xml
sudo virsh autostart moodle
sudo virsh start moodle
cd ~
wget "${LATEST/tag/download}""/$SCORM_TEMPLATE"
chmod +x $SCORM_TEMPLATE
./$SCORM_TEMPLATE /home/$USER/cylms/

# 16. Get CyPROM
cd ~
git clone https://github.com/crond-jaist/cyprom.git
sudo apt -y install python-msgpack

# 17. Get CyTrONE
cd ~
git clone https://github.com/crond-jaist/cytrone.git
sudo apt -y install python-passlib
cd cytrone/scripts/
```

Figure D.3: CyTrONE Installation Script 3



```
cp -a CONFIG.dist CONFIG
sed -i "s/172\.16\.1\.7/$IP/g" CONFIG
sed -i "s/172\.16\.1\.7/$IP/g" ~/cytrone/database/users.yml

# 18. Setup Moodle VM
until ssh -o BatchMode=yes -o ConnectTimeout=5 -o StrictHostKeyChecking=no
-o PubkeyAuthentication=no -o PasswordAuthentication=no -o
KbdInteractiveAuthentication=no -o ChallengeResponseAuthentication=no
$MOODLE_VM_IP 2>&1 | grep "Permission denied"; do
    echo "Waiting for Moodle VM to come online..."
    sleep 1
done  # test whether Moodle VM is up

echo "root@$MOODLE_VM_IP (Moodle VM) password can be found in user guide."
ssh-copy-id root@$MOODLE_VM_IP
ssh root@$MOODLE_VM_IP 'sed -i
"s/https:\/\/localhost/https:\/\/'"$IP"':8081/g"
/var/www/html/moodle/config.php; systemctl restart httpd; exit'

echo "CyTrONE installation completed!"
```

Figure D.4: CyTrONE Installation Script 4

Appendix E

OTnetic User Stories

E.1 Software

ID: 1-S	
Priority: 1 - Must have	
User story:	As a training participant, I want to be able to take the role of an adversary as well as a defender, so I can understand more of what is happening on both sides of a cyber attack.
Description:	The software will consist of two parts; (1) a cyber range with practical tasks and challenges, and (2) a part where information is provided and questions are asked in order for the participant to reflect on what they have learned. These parts are tightly connected and one cannot be completed without the other.
Acceptance criteria:	Given that the user is participating in the training program. When the participant is using the cyber range. Then the participant should either attack or defend a given virtual machine instance depending on the module.

Table E.1: User Story 1-S

ID: 2-S	
Priority: 2 - Must have	
User story:	As a user, I want to be able to access the system remotely, so training can be performed at any time during the day.
Description:	It must be possible for users to access the training program remotely.
Acceptance criteria:	Given that the user is working from home. When the user needs to use the training program. Then the user should be able to access the training program.

Table E.2: User Story 2-S

ID: 3-S	
Priority: 3 - Must have	
User story:	As a moderator/instructor, I want to be able to customize the cyber range according to the users' needs, so that the training is targeted against the appropriate audience.
Description:	Cyber range creation and destruction must be possible by utilizing a script and a template specifying the requirements for the cyber range.
Acceptance criteria:	Given that the cyber range is part of the training module. When the instructor launches a new cyber range instance. Then the instructor must be able to customize it according to the module requirements.

Table E.3: User Story 3-S

ID: 4-S	
Priority: 4 - Must have	
User story:	As an administrator/moderator, I want to be able to manage multiple users and enroll them in different courses, so that they receive training relevant for their situation and knowledge level.
Description:	Cyber range creation and destruction must be possible by utilizing a script and a template specifying the requirements for the cyber range.
Acceptance criteria:	Given that there are several users from different organizations with different knowledge and experiences. When the users are using the training program. Then they should receive training that is most relevant for their needs.

Table E.4: User Story 4-S

ID: 5-S	
Priority: 5 - Must have	
User story:	As a participant, I want to be able to perform the training at any time of the day, so that I can complete my critical work before training.
Description:	The training program must be available when the participant requests access.
Acceptance criteria:	Given that a user has a busy day at work. When the user is supposed to perform training. Then the user should be able to perform the training at a convenient time.

Table E.5: User Story 5-S

ID: 6-S	
Priority: 6 - Must have	
User story:	As a moderator/instructor, I want to be able to create new training modules following a standard format, so that I do not have to know the system intimately to create more training content.
Description:	It should be possible to create new training modules with unique training material and practical challenges. Module creation should follow a standard format, such as yaml.
Acceptance criteria:	Given that there is a need for new training content. When the instructor creates new training content. Then the format of the training content should follow a standard format to save time.

Table E.6: User Story 6-S

ID: 7-S	
Priority: 7 - Should have	
User story:	As a training participant, I want to be able to see my progress and how well I am doing compared to the other training participants, so that I can get better idea of what I need to improve. As an instructor, I want to be able to see how well the training participants are doing, so that I can get a better idea of how effective the training is and if a training module needs to be improved/revised.
Description:	The training program will save the participant's progress so they can continue if an error occurs.
Acceptance criteria:	Given that a user has a busy day at work. When the user is supposed to perform training. Then the user should be able to perform the training at a convenient time.

Table E.7: User Story 7-S

ID: 8-S	
Priority: 8 - Should have	
User story:	As an instructor, I want the user to perform the training using a single solution, so that I do not have to account for multiple solutions when creating and delivering the training content.
Description:	The provided training solution should be a single solution that easily deployable without depending on external frameworks.
Acceptance criteria:	Given that a user is supposed to use OTnetic for cyber training. When they are training on a given module. Then the module should not be dependent on other frameworks that are not included in OTnetic.

Table E.8: User Story 8-S

ID: 9-S	
Priority: 9 - Should have	
User story:	As an instructor, I want to be able to destroy and create a cyber range instance based on a template, so that I do not have to waste time doing it manually.
Description:	There should be a script that can be utilized in order to create and destroy cyber ranges easily. The script will utilize a template written in the "yaml" format. The template specifies the amount of virtual guest machines in the range, IP addresses, OS' etc.
Acceptance criteria:	Given that a cyber range needs to be re-instantiated or created for the first time. When the instructor destroys or create a new cyber range instance. Then the cyber range details should be specified in a template to save time upon destruction and creation of cyber range instances.

Table E.9: User Story 9-S

ID: 10-S	
Priority: 10 - Should have	
User story:	As an instructor, I want the cyber range instance to have its own subnet, so that I can launch multiple virtual machine instances that can communicate with each other. (Possible to represent an infrastructure with multiple machines)
Description:	The cyber range will have its own subnet and virtual machines in the range will have to ability to communicate with each other using tools such as ping and ssh.
Acceptance criteria:	Given that there are multiple virtual machines in the cyber range. When a user is supposed to attack a machine or defend from an attacking machine. Then the machines must have the ability to communicate with each other on the same subnet.

Table E.10: User Story 10-S

ID: 11-S	
Priority: 11 - Should	
User story:	As a user, I want the cyber range application to only allow certain commands, so that the cyber range training easier to understand and use.
Description:	Interview data suggests that the current cyber security knowledge level of the target group is limited. Therefore, the initial module and CLI-command selection will be limited through the use of a python application.
Acceptance criteria:	Given that a user is unfamiliar with a CLI-interface. When the user is entering the cyber range. Then the user should not be overwhelmed with too many options and to restrain the user from executing arbitrary commands causing the application to crash.

Table E.11: User Story 11-S

ID: 12-S	
Priority: 12 - Should have	
User story:	As a training participant, I want to be able to save my progress in the cyber range, so that I do not have start from scratch if the application closes or crashes.
Description:	The cyber range will include functionality that allows a user to quit and continue their training without resetting their progression in the cyber range narrative.
Acceptance criteria:	Given that the user manages to close or crash the cyber range application. When the user tries to restart the application. Then the user should continue from where the user left off rather than start from the beginning.

Table E.12: User Story 12-S

ID: 13-S	
Priority: 13 - Could have	
User story:	As a user, I want to be able to cooperate with other users during the training, so that I can discuss a particular challenge/exercise with a colleague and share our solutions.
Description:	A social platform could be included in the learning management system that would allow users to communicate with each other using chat functionality.
Acceptance criteria:	Given that multiple users are training simultaneously. When using a specific module. Then they should be able to ask each other for help as this will allow participants to share experiences and opinions.

Table E.13: User Story 13-S

E.2 Training Content

ID: 1-TM	
Priority: 1 - Must have	
User story:	As a manager, I want an effective alternative to conventional training methods, so that I can increase the cyber security knowledge of my employees in order to improve the security posture of my organization. As a participant, I want an alternative training program that is more effective than lectures, and more fun and motivating to use than traditional training methods.
Description:	The training program should be be more effective than traditional training methods in terms of the user's ability to gain knowledge and practical skill related to various cyber security concepts such as authentication.
Acceptance criteria:	Given the participant requires additional cyber security training. When the participant completes a module of the training program. Then the participant's knowledge the module's security knowledge is greater than before they completed the module.

Table E.14: User Story 1-TM

ID: 2-TM	
Priority: 2 - Must have	
User story:	As a training participant, I want the training content to include elements from gamification so that the training becomes more motivating and interesting.
Description:	The training program must include elements of gamification that will make the program more motivating to use, while increasing the participant's learning output.
Acceptance criteria:	When a participant is performing the training program. Given the participant wants to receive fun and motivating training content. Then the training program should provide elements of game design, as this has proven to create more motivating and engaging training.

Table E.15: User Story 2-TM

ID: 3-TM	
Priority: 3 - Must have	
User story:	As a training participant, I want the training to include problem solving, to make the participants more focused while training.
Description:	The training program will include challenges that will be increase the participant's ability to perform problem solving tasks. Using critical thinking in order to solve problems will help create transferable knowledge.
Acceptance criteria:	When an instructor is creating a new training module. Given that the training module will be used to create transferable knowledge. Then the training module should provide exercises that require some degree of problem solving, in order to make the knowledge acquired through training applicable in other scenarios.

Table E.16: User Story 3-TM

ID: 4-TM	
Priority: 4 - Must have	
User story:	As a participant, I want the training program to provide a difficulty level that reflects my prior knowledge on a given topic related to cyber security.
Description:	The cyber security training program should allow for inclusion of multiple modules related to different different subjects. Modules will have different difficulty levels in order to suit the abilities and weaknesses of each participant.
Acceptance criteria:	Given the participant only has basic knowledge of cyber security concepts. When the participant utilizes the training program. Then the user will be able to select a relevant module with an easy difficulty level.

Table E.17: User Story 4-TM

ID: 5-TM	
Priority: 5 - Must have	
User story:	As a participant, I want to be able to receive instructions and test my knowledge while I am acquiring practical skills in the cyber range.
Description:	The training program should provide relevant information and instructions that will help the user complete the cyber range training. There should be a strong connection between practical tasks issued in the cyber range and the information and questions provided in the quiz part of the training program.
Acceptance criteria:	Given the participant is using the training program. When the participant is performing practical tasks in the cyber range. Then the participant will receive information and questions related to their challenge in the information/quiz portion of the training program.

Table E.18: User Story 5-TM

ID: 6-TM	
Priority: 6 - Must have	
User story:	As a participant, I want to learn about good and bad security practices in order to prevent security incidents in the future.
Description:	The training program should show the participants examples of good and bad security practices. This will provide them with a better understanding security issues, while equipping them with the necessary skills to avoid bad practices and employ good practices.
Acceptance criteria:	Given the participant is using the training program. When the participant is receiving information and performing tasks. Then the participant is provided with examples and tasks illustrating good and bad security practices.

Table E.19: User Story 6-TM

ID: 7-TM	
Priority: 7 - Must have	
User story:	As a user, I want the training content I am provided with to be written in Norwegian, as that is my native language and the language used in my workplace.
Description:	The training program must be written in Norwegian, as the target group is employees working in the Norwegian energy sector. It is important that the target audience fully understands the information they are given. In order to avoid misunderstandings and confusion. The training content and program will be provided in the users native language.
Acceptance criteria:	When the user is enrolled in the training program. Given the user is Norwegian. Then the training content should be provided in Norwegian.

Table E.20: User Story 7-TM

ID: 8-TM	
Priority: 8 - Must have	
User story:	As a manager, I want the information given in training program to reflect the current security guidelines issued by NSM.
Description:	The training program should take NSM's security guidelines into account and reflect the current recommendations provided by NSM.
Acceptance criteria:	Given the administrator is creating a new module. When a new module is under development. Then the information should reflect the current recommendations provided by NSM.

Table E.21: User Story 8-TM

ID: 9-TM	
Priority: 9 - Must have	
User story:	As a participant, I want increasingly difficult challenges.
Description:	In addition to providing the ability to implement different modules, each module in the training program should have challenges of increasing difficulty in order to push the user learn more and build on the skills and knowledge they acquire through the module.
Acceptance criteria:	Given the participant is using the training program. When the participant completes a challenge in the cyber range. Then the next challenge should be slightly more difficult than the previous challenge.

Table E.22: User Story 9-TM

ID: 10-TM	
Priority: 10 - Must have	
User story:	As a participant, I want to see how cyber attacks are performed and gain a greater understanding how security vulnerabilities are exploited.
Description:	The cyber range platform should provide participants with examples that illustrate and visualize cyber attacks related to the module they are training on.
Acceptance criteria:	Given the participant is using the training program. When the participant is performing a challenge related to attacks in the cyber range. Then the participant is able to perform the attack and see how it works and what the result is.

Table E.23: User Story 10-TM

ID: 11-TM	
Priority: 11 - Should have	
User story:	As a training participant, I want to be able experience how it is to be the adversary in cyber operation and perform different cyber attacks, so that I can understand how bad security practices allow for attacks by adversaries.
Description:	The cyber range platform should provide participants with an understanding of the adversary's perspective, and how poor security practices can be exploited.
Acceptance criteria:	Given the participant is using the training program. When the participant is using the cyber range. Then the participant is able to complete challenges related to red-team activities.

Table E.24: User Story 11-TM

ID: 12-TM	
Priority: 12 - Should have	
User story:	As a participant, I want the training program to be fun and enjoyable so that my motivation to complete the program is greater.
Description:	The training program should be fun to participate in. By using gamification elements such as a point system, increasingly difficult challenges, visual feedback etc. the program will be more enjoyable than traditional training methods.
Acceptance criteria:	Given the participant requires training. When the participant is using the training program. Then the participant should find the program fun to participate in.

Table E.25: User Story 12-TM

ID: 13-TM	
Priority: 13 - Should have	
User story:	As a training participant, I want to learn different tools and techniques related to different security topics, so that I use these tools to improve my understanding of security.
Description:	The training program should include different tools and techniques used by adversaries in order to create a better understanding of security issues.
Acceptance criteria:	Given the participant is using the training program. When the participant is performing practical challenges. Then the participant should given the ability to utilize real tools and techniques.

Table E.26: User Story 13-TM

ID: 14-TM	
Priority: 14 - Should have	
User story:	As a training participant, I want parts of the training to be story-based, so the training is more interesting and fun.
Description:	The training program should be story-based. Information and challenges provided in the training program should follow a cohesive realistic narrative.
Acceptance criteria:	Given that there is a need for new training content. When the instructor creates additional training content. Then the training content should be story-based.

Table E.27: User Story 14-TM

ID: 15-TM	
Priority: 15 - Could have	
User story:	As a training participant, I want the training to include knowledge that I can use in my personal life, so that I get motivated to learn more and that the knowledge gained can be applied outside of work.
Description:	It is desirable that knowledge and skills can be transferred to the participant's personal life, resulting in increased personal security in addition to better security practices in their work lives.
Acceptance criteria:	Given that a participant is using the training program. When they are introduced to new security concepts and various techniques. Then the knowledge gained by the participant should be applicable in their personal lives.

Table E.28: User Story 15-TM

Appendix F

Range Instantiation

```
---
- host_settings:
  - id: host_1
    mgmt_addr: localhost
    virbr_addr: 192.168.122.1
    account: cyuser

- guest_settings:
  - id: red
    basevm_host: host_1
    basevm_config_file: /home/cyuser/images/basevm.xml
    basevm_type: kvm
    tasks:
    - install_package:
      - package_manager: yum
        name: python3
    - copy_content:
      - src: /home/cyuser/cyber_range_program/OTnetic
        dst: /home/trainee01

  - id: blue
    basevm_host: host_1
    basevm_config_file: /home/cyuser/images/basevm.xml
    basevm_type: kvm
    tasks:
    - add_account:
      - account: blue
        passwd: n8sv4yo7m9
```

```
- clone_settings:
  - range_id: 123
    hosts:
    - host_id: host_1
      instance_number: 1
      guests:
      - guest_id: red
        number: 1
        entry_point: yes
      - guest_id: blue
        number: 1
      topology:
      - type: custom
        networks:
        - name: office
          members: red.eth0, blue.eth0
```

Appendix G

Evaluation Metrics

The following is a list of evaluation metrics for each category, which are illustrated in figure 5.11. The list contains the metrics, with a short explanation for each metric. Based on these metrics, questions were developed for the questionnaire where respondents were asked to agree or disagree on a 5-point Likert scale.

Software

1. *Deployment:* is the program easy to implement by the client organization?
2. *Usability:* is the program easy to utilize by participants?
3. *Stability:* does the program function as expected during the training session?
4. *Motivation:* does the training program provide training in a motivating and engaging fashion?

training Content

1. *Motivation:* does the training content provide information in a motivating and engaging fashion?
2. *Attitude:* do the participants have changed attitudes towards the importance of security?
3. *Knowledge:* does the training content provide new knowledge?
4. *Relevance:* do the participants find the material relevant for their role?
5. *Difficulty:* is the training content too difficult or too easy?

Appendix H

Interview Guide for OT-personnel in the Norwegian Energy Sector (Norwegian)

Hensikten med dette intervjuet er å få et bedre bilde av hvordan de som jobber med OT ser på cybersikkerhet og om OT-ansatte får noe form for opplæring, kursing, etc. innen cybersikkerhet. Før vi begynner vil vi opplyse om at svarene du gir oss ikke vil knyttes til ditt navn. Hvis vi spør om noe som gjør det vanskelig å unngå sensitiv informasjon, er det bare å si ifra slik at vi kan unngå dette.

H.1 Current Status of Training

1. Kan du fortelle meg om hva slags opplæring OT-personell får med tanke på IT-sikkerhet?
2. Hvordan tror du at denne treningen kan bli bedre?
3. Føler du at disse treningsprogrammene gir et godt bilde av sikkerhetsproblematikken knyttet til informasjonsteknologi?
4. Vet du om bedriften du jobber i har interne sikkerhetsregler for driftssystemer / retningslinjer IT-sikkerhet (f.eks passordregler, acceptable use policy)?
5. I hvilken grad opplever du at andre ansatte i bedriften følger disse reglene og retningslinjene?

H.2 Attitudes Towards Information Security

Noen mener at det er et tydelig skille mellom hva de som jobber med OT og IT er opptatt av med tanke på sikkerhet (security/safety) og arbeidsoppgaver.

1. Tror du kollegaene dine ville vært enige i denne påstanden?

2. Hva tror du de ansatte du jobber med tenker om at OT-ansatte eller andre som ikke jobber i IT-avdelingen kan påvirke sikkerheten i bedriften? Tror du de fleste ansatte ser på dette som et felles ansvar?

3. Tror du at de fleste i bedriften har ferdigheter og kunnskaper som gjør at de kan hjelpe til i arbeidet med å sikre bedriften (eks. oppdage phishing eller feil verdier i SCADA)?

4. Tror du at ansatte er klare over at det er sårbarheter i OT-systemer som kan benyttes av trusselaktører hvis de finnes (eks. ondsinnede hackere)? Vet du om noen slike sårbarheter som har blitt oppdaget og fikset tidligere?

5. Hva tror du er den mest kritiske sikkerhetstrusselen (ikke safety) i OT-verden? Oppfølging: Hva slags cyber-angrep mener du hadde hatt størst innvirkning på bedriften/samfunnet? Hva slags cyber-angrep tror du er mest vanlig?

6. Har du eller noen andre opplevd en sikkerhetshendelse i bedriften du jobber i? Hvordan ble dette håndtert?

H.3 Opinions On Development of a New Training Program

Under masteroppgaven skal vi utforme et treningsprogram spesielt laget for de som jobber med OT i energisektoren. For å kunne oppnåønsket resultat trenger vi litt hjelp fra de som skal få treningen. Produktet vi forventer å utforme/bygge vil mest sannsynlig bli i form av et rammeverk eller et program/applikasjon som bygger på prinsipper fra simulering og "gamifisering" med forskjellige oppgaver og utfordringer.

1. Tror du at andre i bedriften som ikke jobber i IT-avdelingen synes dette med IT og sikkerhet er vanskelig eller forvirrende?

2. Hva tenker du om å gjennomføre et treningsprogram hvor du får praktiske oppgaver og ser IT-sikkerhet fra begge sider (forsvar/angrep)? Tror du andre hadde vært positive til dette?

3. Er det noe spesielt du ønsker å lære mer om innen IT-sikkerhet, eller noe du tror det er behov for i bedriften/sektoren?

Appendix I

Interview Guide for Security Consulting Company (Norwegian)

I.1 Current Status of Training

1. Kan du fortelle meg om hvordan opplæring innen cybersikkerhet fungerer i bedriftene du jobber med?
2. Hva slags trening tilbyr dere til nye ansatte som skal jobbe med sikkerhet?
3. Har bedriftene klare planer for roller og ansvarsfordeling dersom en sikkerhetshendelse forekommer?
4. Føler du at disse treningsprogrammene gjør en tydelig merkbar forskjell i forbindelse med kunnskap og forberedthet?
5. Føler du at disse treningsprogramme mangler noe i forhold til bevissthet om sikkerhetsproblematikk eller teknisk forberedelse?
6. Tilbyr NC-Spectrum noe form for opplæring innen sikkerhet for deres kunder?
7. Hvilken form for trening har opplevd at er mest kostnadseffektiv?

I.2 Security Requirements in the Energy Sector

1. Er det noen spesifikke eller unike sikkerhetskrav som er felles for bedriftene i energisektoren? (eller i annen kritisk infrastruktur?)
2. Er det mange krav som skiller seg veldig fra hverandre, eller har de stort sett like sikkerhetsutfordringer?
3. Bruker disse bedriftene betydelig mer ressurser påcybersikkerhet enn andre bedrifter?
4. Kan du si noe om sikkerhetsproblemer eller -situasjoner som er unike for bedrifter i

denne sektoren? (f.eks med tanke påat de drifter CPS-er, ansvar for sikkerhet, innvirkning påsamfunnet osv)

5. Anser du disse bedriftene som attraktive mål for cyberkriminelle eller andre ondsinnede aktører?

I.3 Attack Simulation

1. Hva slags type angrep forkommer oftest i ditt selskap og dine kunders selskaper? Hva slags type angrep har høyest innvirkning?
2. Benytter dere cyber ranges eller andre former for blue/red team trening (ifm penetrasjonstesting)?
3. Tenker du at åsimulere spesifikke angrepstyper i en kontrollert setting for sikkerhetsspesialister i deres selskap kunne forbedret egenskapene til deltagerne? (gjøre dem mer forberedt påslike angrep i en realistisk setting)
4. Hva tror du kan være utfordrende med en slik treningsmodell?
5. Hva tror du kunne vært fordelaktig med å implementere en slik modell?

I.4 Use of Existing Training Frameworks

1. Bruker dere noen eksisterende rammeverk for trening som er relevant for cybersikkerhet? (Hvis ja: hvilke? Følg opp...)
2. Hvordan har dere tilpasset disse rammeverkene til å passe deres unike behov og sikkerhetskrav?
3. Hva er er deres nåværende fokusområder i rammeverkene og programmene dere bruker? (eks. deteksjon, forhinding, risikostyring etc.)